MX3-RFID Reference Guide

(Microsoft® Windows® CE .NET Equipped)

E-EQ-MX3RFIDRG-A

Notices

LXE Inc. reserves the right to make improvements or changes in the products described in this guide at any time without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, LXE assumes no liability resulting from any errors or omissions in this document, or from the use of the information contained herein. Further, LXE Incorporated, reserves the right to revise this publication and to make changes to it from time to time without any obligation to notify any person or organization of such revision or changes.

Copyright:

Trademarks:

LXE® is a registered trademark of LXE Inc. Sirit is a trademark of Sirit, Inc.

Intel® and Intel XScale are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft®, ActiveSync®, MSN, Outlook®, Windows®, the Windows logo, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

RAM® and RAM Mount™ are both trademarks of National Products Inc., 1205 S. Orr Street, Seattle, WA 98108.

Odyssey® and Funk® are registered trademarks of Funk Software, Inc.

Summit Data Communications, Inc. Summit Data Communications, the Summit logo, and "The Pinnacle of Performance" are trademarks of Summit Data Communications, Inc.

All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

When this manual is in PDF format: "Acrobat® Reader® Copyright © 2006 Adobe Systems Incorporated. All rights reserved. Adobe®, the Adobe logo, Acrobat®, and the Acrobat logo are registered trademarks of Adobe Systems Incorporated." Applies.

Li-Ion Battery

When disposing of the main battery, the following precautions should be observed:
The battery should be disposed of promptly. The battery should not be disassembled or crushed. The battery should not be heated above 212°F (100°C) or incinerated.

Important: This symbol is placed on the product to remind users to dispose of Waste Electrical and Electronic Equipment (WEEE) appropriately, per Directive 2002-96-EC. In most areas, this product can be recycled, reclaimed and re-used when properly discarded. Do not discard labeled units with trash. For information about proper disposal, contact LXE through your local sales representative, or visit www lxe com.

Table of Contents

Illustrations

Chapter 1 Introduction

Overview

The LXE® MX3-RFID mobile device is a rugged, portable, hand-held Microsoft® Windows® CE .NET equipped device capable of wireless data communications.

It is the RFID version of the LXE MX3X Xscale mobile device.

The mobile device can transmit information using a 2.4 GHz radio (with an internally mounted antenna) and it can store information for later transmission wirelessly or via an InfraRed or USB port. The device can be scaled from a limited function batch computer to an integrated RF scanning computer.

The mobile device is horizontally oriented and features backlighting for the display. The touch-screen display supports graphic features and Windows icons that the Windows CE .NET operating system supports. The keys on the keypad are constructed of a phosphorescent material that can easily be seen in dimly lighted areas.

The MX3-RFID has an RFID module permanently attached to the back of the device. The module protects the RFID antenna and tag reader. A passive vehicle cradle is available that has been designed specifically for the MX3-RFID devices deeper back cover.

Device-specific cables are available. The stylus in the Stylus Kit (shipped with each unit) is used to assist in entering data and configuring the unit. Protective film for the touchscreen is available as an accessory.

*Note: Until the main battery and backup battery are completely depleted, the mobile device is **always** drawing power from the main and backup batteries (**On**).*

When to Use This Guide

As the reference for LXE's MX3-RFID mobile device, this guide provides detailed information on its features and functionality. Use this reference guide as you would any other source book – reading portions to learn about the device and it's capabilities, and then referring to it when you need more information about a particular subject. This guide takes you through all aspects of installation and configuration.

Instruction and safety information for the general user are contained in the "MX3-RFID User's Guide."

This chapter, **"Introduction",** describes this reference guide's structure, contains setup and installation instruction, briefly describes data entry processes, and explains how to get help.

Chapter 2 "Physical Description and Layout", describes the function and layout of the configuration, controls, connectors, keypads and the power supply. The passive cradle and the battery charging station are included in this section.

Chapter 3 "System Configuration" takes you through the CE .NET operating system setup and RFID file structure.

Chapter 4 "Wireless Network Configuration" details 2.4GHz radio setup. Configuration for WEP and WPA is included.

Appendix A "Key Maps" describes the keypress sequences for the QWERTY keypad. "Creating Custom Keymaps" is included in this appendix.

Appendix B "Technical Specifications" lists technical and environmental specifications for the mobile device.

Document Conventions

ALL CAPS	All caps are used to represent disk directories, file names, and application names.
Menu | Choice	Rather than use the phrase "choose the Save command from the File menu", this guide uses the convention "choose File | Save".
"Quotes"	Indicates the title of a book, chapter or a section within a chapter (for example, "Document Conventions").
< >	Indicates a key on the keypad (for example, <Enter>).
📖	Indicates a reference to other documentation.
ATTENTION	Keyword that indicates vital or pivotal information to follow.
⚠	Attention symbol that indicates vital or pivotal information to follow. Also, when marked on product, means to refer to the manual or user's guide.
△	International fuse replacement symbol. When marked on the product, the label includes fuse ratings in volts (v) and amperes (a) for the product.
Note:	Keyword that indicates immediately relevant information.
CAUTION ⚠	Keyword that indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
WARNING ⚠	Keyword that indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
DANGER ⚠	Keyword that indicates a imminent hazardous situation which, if not avoided, will result in death or serious injury.

Related Manuals

Available for download from the LXE Manuals CD or the LXE ServicePass website.

MX3-RFID User's Guide - contains general user information and instruction. An abbreviated user's guide (LXEbook – MX3-RFID User's Guide) is available.

MX3 Cradle Reference Guide – contains technical information, installation and operating instruction relating to the MX3-RFID Passive Vehicle Mount cradle.

MX3 Multi-Charger User's Guide - contains technical information and operating instruction for the MX3 Multi-Charger Plus main battery stand-alone charging/analyzing device.

Integrated Scanner Programming Guide - set up the integrated SE923 or SE955 scanner barcode reading parameters. The SE923 scanner was replaced with the SE955 scanner in July 2006. Both scan engines are represented in the programming guide.

LXE Security Primer – contains technical information and setup instructions for wireless network configurations at the access point level.

RFTerm Reference Guide – terminal emulation programming guide.

RFID

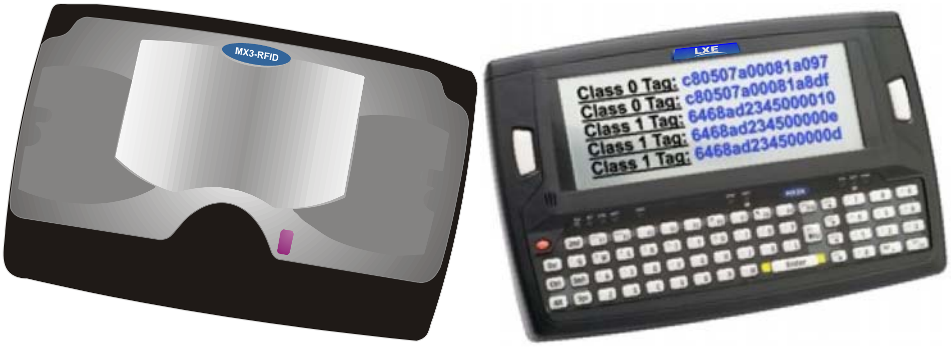

MX3-RFID
LXE
Class 0 Tag: c80507a00081a097
Class 0 Tag: c80507a00081a8df
Class 1 Tag: 6468ad2345000010
Class 1 Tag: 6468ad234500000e
Class 1 Tag: 6468ad234500000d

Figure 1-1 MX3-RFID Device

Radio frequency identification, or RFID, is a generic term for technologies that use radio waves to automatically identify individual items. The individual items identified/read by a RFID reader contain a tag (also known as an electronic label or transponder). Unlike barcodes that must be read by a beam passing over the barcode, RFID tags do not have to be in the line-of-sight of the reader before the reader can collect the data from the tag but they do need to be within the established "read" distance from the RFID module.

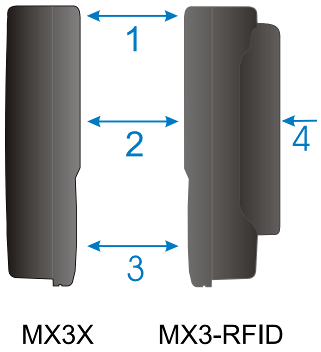
When the RFID Read button is pressed, the tag reader turns on and the MX3-RFID beeps once if the tag (or tags) was located and read successfully. The reader turns off at a predetermined time limit after a good read or a failed read. The data gathered from the tag is sent to a user-specified storage area (i.e. open text file) for further handling e.g. sent to the host using wired or wireless networking. See the section titled "How To" for instruction.

There may be a buzz sound during the time the reader is "searching and reading" if the RFID reader is configured to buzz during a read cycle.

Note: The RFID Module also has a hand strap. Location and attach points are different from the standard MX3X hand strap. MX3-RFID devices are shipped with the hand strap already installed.

Note: Always store unused devices with a fully charged main battery installed. LXE recommends an in-use mobile device be frequently connected to an external power source to retain optimum power levels in the main battery and the backup battery. After the backup battery and main battery are depleted (dead), then when a fully charged main battery is installed, and the device powered On again, the mobile device reverts to the last saved default (or factory) values. Follow the steps in "Getting Started".

MX3X vs MX3-RFID Chart



1 Endcap

2 Touchscreen

3 Keypad

4 RFID Module

MX3-RFID Capability/Function	MX3-RFID
Integrated Scanner port (SE923 or SE955 see note)	x
RFID Reader	x
USB Client RS232 port	x
Cisco 802.11 Client	x
Passive Cradle	x
Intel XScale^{TM} PXA255 400MHz CPU	x
128M Flash / 128M RAM or greater	x
Windows CE .NET 4.2	x
RFTerm / Barcode Wedge	x
JAVA support	x
63 Key QWERTY Keypad, two large user mappable scan keys	x
640 x 240 1/2 VGA LCD 6" diagonal - color	x
Touchscreen and stylus	x
10.8V, 2200mAh Li-Ion battery pack	x
IR Port	x
Handstrap	x
Holster	x
IP65	x
Available in US and Canada	x

- The SE 923 short range laser scanner was replaced by the SE 955 laser scanner in July 2006.
- MX3-RFID mobile devices are available in the USA only.
- The RFID Module has a hand strap. Location and attach points are different from the standard MX3X hand strap. MX3-RFID devices are shipped with a hand strap already installed.

Components

Front and Back Views

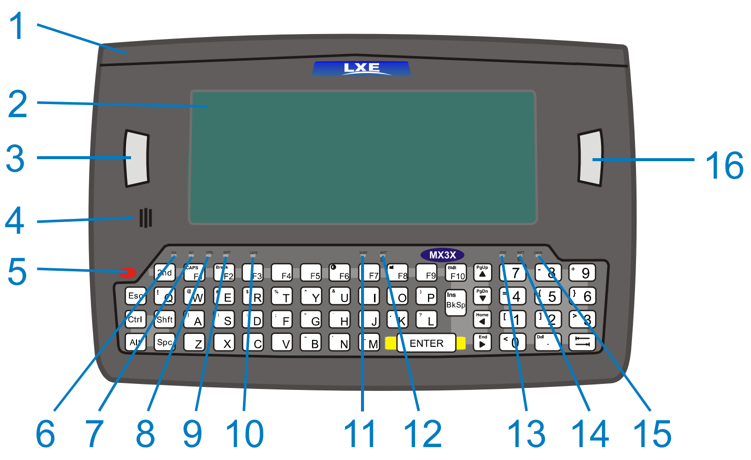


Figure 1-2 Front

1	Endcap	9	Shift LED
2	Display	10	Caps LED
3	Scan, Enter or Field Exit (programmable)	11	Scanner LED
4	Beeper	12	Backup Battery LED
5	On/Off Button	13	Status LED
6	2nd LED	14	Main Battery LED
7	Alt LED	15	Charger LED
8	Ctrl LED	16	Scan or Enter (programmable)

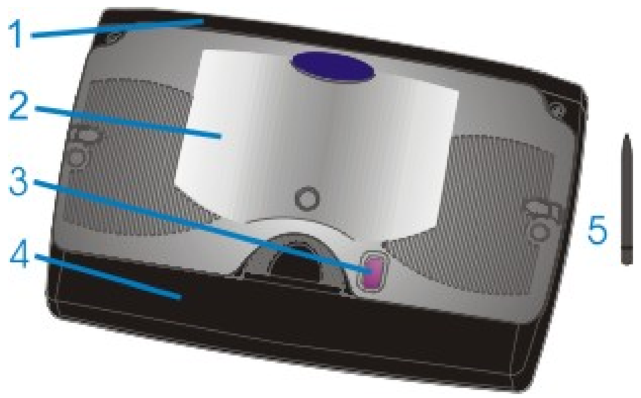


Figure 1-3 Back

1	Endcap	4	Main Battery
2	RFID Enclosure	5	Stylus
3	IR Port (Com 2 Port)		

Endcap Options

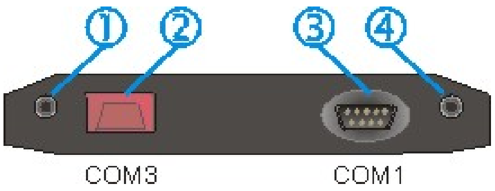
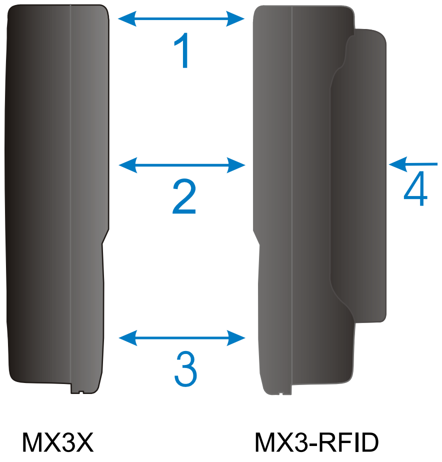


Figure 1-4 Endcaps

1	DC Power Jack	3	Serial Com 1 or USB Client Port
2	Laser Scanner Aperture	4	Audio Jack

RFID Module



1 Endcap w/Laser Scanner

2 Touchscreen

3 Keypad

4 RFID Module

Figure 1-5 Side View

Battery Well Vent Aperture

Caution

The vent aperture in the battery well should never be blocked with any device *other than an approved LXE main battery*. The vent aperture functions to relieve any heat or pressure that may build up in the mobile device during everyday use.

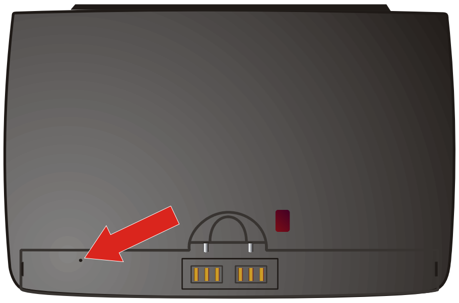


Figure 1-6 Vent Aperture in Battery Well – Do Not Cover

If the vent hole is covered by an object, e.g. a tracking label, other than an approved LXE main battery, the touch screen may be damaged. If damage occurs to the touch screen, please contact your LXE representative for the process to follow when returning the device to LXE for repair.

Note that the MX3-RFID has a dust and water protection enclosure rating of IEC 60529 compliant to IP65.

Getting Started

Note: When your mobile device is pre-configured, the radio, PCMCIA card and endcaps are assembled by LXE to your specifications.

This section's instructions are based on the assumption that your new MX3-RFID is pre-configured and requires only accessory installation (e.g. stylus) and a power source. LXE recommends that installation or removal of accessories be performed on a clean, well-lit surface. When necessary, protect the work surface, the mobile device, and components from electrostatic discharge.

Use this guide as you would any other source book – reading portions to learn about the device, and then referring to it when you need more information about a particular subject. This guide takes you through an introduction to and operation of the MX3-RFID.

In general, the sequence of events is:

1. Insert a fully charged battery and press the Power button.
2. Connect an external power source to the device (if required).
3. If the screen does not automatically display, press the Power button.
4. Adjust screen display, audio volume and other parameters if desired.

Troubleshooting

Touchscreen is not accepting stylus taps or need recalibration.	Press <Ctrl>+<Esc> to force the Start Menu to appear. Use the tab, backtab and cursor keys to move the cursor from element to element.

Note: The MX3-RFID does not support tethered scanners. Do not connect a tethered scanner cable to a USB-C labeled endcap port. These ports cannot power a tethered scanner.

Insert Main Battery

Press the Power button after the battery is inserted into the battery compartment.

Note: ***New batteries must be charged prior to first use****. This process takes up to four hours in an LXE Multi-Charger Plus and eight hours with an external power source connected to the power jack on the endcap of the mobile device.*

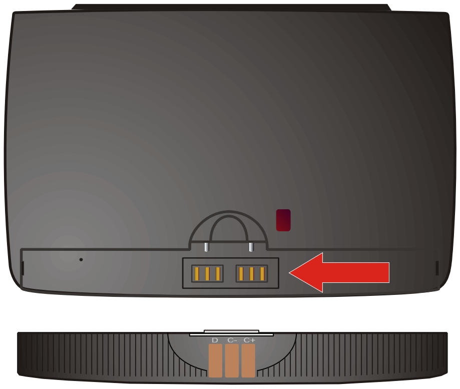


Figure 1-7 Battery Contacts and Main Battery

The Main Battery compartment is located at the bottom of the back of the computer. The arrow in the top figure points to the battery contacts in the battery well. The bottom figure shows the battery charger contacts on the back of the main battery.

Place the battery in the compartment, making sure the side of the battery with six contacts matches up with the battery contacts in the battery well. Do not slide the battery sideways into the battery well.

Firmly press the battery into the well until the Retaining Clip on the battery clicks. The battery is now securely fastened to the computer. The computer draws power from the battery immediately upon successful connection.

Note: Do not cover the vent aperture (located in the left side of the battery well) in the battery well with anything other than the main battery.

Check Battery Status

Tap the **Start | Settings | Control Panel | Power** icon. Main and backup battery level, status and Power Scheme timeout setting options are displayed.

About Lithium-Ion Batteries

Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the mobile device is always ‘on’ even when in the Suspend state and draws battery power at all times. Use the **Start | Settings | Control Panel | Power | Battery** tab to check the battery status and power reading.

Always replace the used main battery with a fully charged main battery. The Battery Low Warning LED illuminates red at approximately 35% of power left in the main battery. You need to determine the point at which battery life becomes unacceptable for your business practices and replace the main battery before that point.

Optional Devices

Each MX3-RFID mobile device is shipped with a handstrap, installed by LXE prior to shipping. A standard MX3X handstrap is not to be used with the MX3-RFID device. Replacement MX3-RFID handstraps can be ordered from LXE (see “Accessories”).

Attach the Stylus Clip (Optional)

Carefully remove the paper backing from the Stylus Clip sticky. Firmly press the sticky side of the clip onto the mobile device and hold in place for 15 seconds. Thread the tether through the end of the stylus and tie the ends firmly to the Stylus Clip so that the ends don’t interfere with placing the stylus in the Stylus Clip. Place the stylus in the Stylus Clip when not in use.

An extra stylus or replacements can be ordered from LXE. See the section titled “Accessories”.

Apply the Protective Film to the Display (Optional)

First, clean the display of fingerprints, lint particles, dust and smudges. See section titled “Cleaning the Glass Display/Scanner Aperture”.

Remove the protective film from it’s container. Remove any protective backing from the film sheet by lifting the backing from a corner of the film. Discard the backing.

Apply the film to the screen starting at one side and smoothing it across the display. If air bubbles appear, raise the film slightly and continue smoothing the film across the display until it covers the glass surface of the display.

If dust, lint or smudges are trapped between the protective film and the glass display, remove the protective film, clean the display and apply the protective film again.

Connect External Power Supply (Optional)

The LXE-approved AC Power Adapter is only intended for use in a 25ºC (77ºF) maximum ambient temperature environment.

There are three external power supplies available for the mobile device and the MX3 desktop cradle:

- US AC/DC 12V Power Supply
- Cigarette Lighter Adapter
- International AC/DC 12V Power Supply

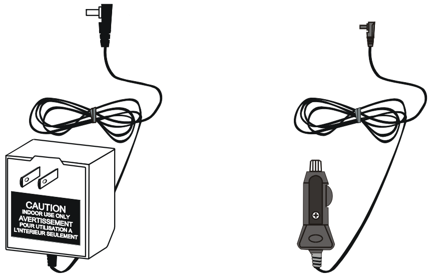


Figure 1-8 US AC/DC 12V Power Supply and Automotive Power Adapter

Figure 1-9 International AC/DC 12V Power Supply

The DC power jack is located on the endcap.

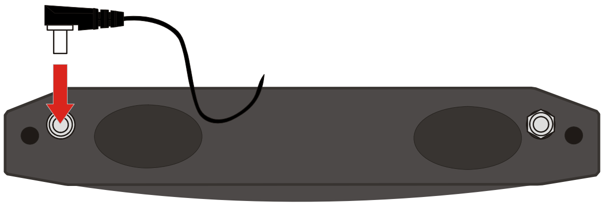


Figure 1-10 Connect External Power Supply

1. Insert the barrel connector into the power jack on the endcap and push in firmly.

2. The CHGR LED above the keypad illuminates when the mobile device is receiving external power through the power jack.

Note: When the mobile device is receiving external power the CHGR LED above the keyboard is illuminated.

See section titled “LED Functions” for explanations of the LEDs for the BATT B and BATT M illuminations.

Connect Audio Jack (Optional)

The audio jack is located on the endcap.

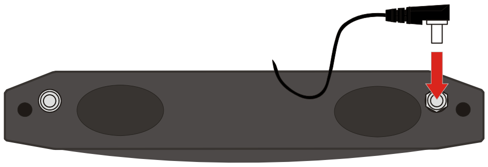


Figure 1-11 Connect Audio Jack

Insert the 2.5mm barrel end of the connector into the audio jack on the endcap and push the connector in firmly. See section titled “Set the Audio Speaker Volume”.

Note: The audio option draws power from the battery. The speaker is disabled when a headset is plugged into the audio jack.

Power Button

Note: Refer to the section titled “Power Modes” later in this chapter for information relating to the power states of the mobile device.

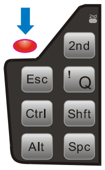


Figure 1-12 Power Button

The power button is located above the ESC key on the keypad. When a battery is inserted in the mobile device press the Power button.

Quickly tapping the Power button places the device immediately in Suspend mode. Quickly tapping the Power button again, or touching the screen, immediately returns the device from Suspend.

When the Windows desktop is displayed or an application begins, the power up (or reboot) sequence is complete.

Please refer to the section titled “Power Modes” later in this guide for a list of the kinds of activities (Primary Events) that will return the device from Suspend Mode.

Restart Sequence

Tap **Start | Run,** then type **warmboot** in the textbox and press Enter. If the touchscreen is not accepting taps or needs recalibration, press <Ctrl>+<Esc> to force the Start Menu to appear.

When the Windows CE. NET desktop is displayed or an application begins, the power up (or restart) sequence is complete. If you have previously saved your settings, they will be restored on reboot.

Any RFID tag data retrieved and not saved is lost during a reboot or reset.

Tapping the Touchscreen with a Stylus

Note: Always use the point of the stylus for tapping or making strokes on the touchscreen. Never use an actual pen, pencil, abrasive or sharp object to write on the touchscreen.

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. Firmly press the stylus into the stylus holder when the stylus is not in use.

Like using a mouse to left-click icons on a desktop computer screen, using the stylus to tap icons on the touchscreen is the basic action that can:

- Open applications
- Choose menu commands
- Select options in dialog boxes or drop-down boxes
- Drag the slider in a scroll bar
- Select text by dragging the stylus across the text
- Place the cursor in a text box prior to typing in data or retrieving data using the integrated barcode scanner or an input/output device connected to the serial port.

An extra or replacement stylus can be ordered from LXE. See the section titled “Accessories” for the stylus part number.

Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:

- Press Tab and an Arrow key to select a file.
- Press Shift and an Arrow key to select several files.
- Once you’ve selected a file, press Alt then press Enter to open its Properties dialog.
- Press 2nd then press numeric dot to delete a file.
- To force the Start menu to display, press Ctrl then press Esc.

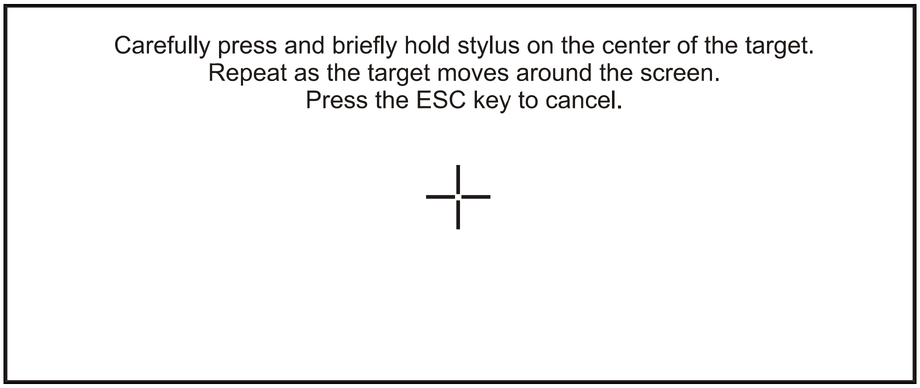
Touchscreen Calibration

If the touchscreen is not responding properly to pen touch taps, you may need to recalibrate the touchscreen. Recalibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

If the touchscreen is not accepting taps or needs recalibration, press <Ctrl>+<Esc> to force the Start Menu to appear.

To recalibrate the screen, select **Start | Settings | Control Panel | Stylus | Calibration** tab.

To begin, tap the Recalibrate button on the screen with the stylus.



Carefully press and briefly hold stylus on the center of the target.
Repeat as the target moves around the screen.
Press the ESC key to cancel.

Figure 1-13 Touchscreen Recalibration

Follow the instructions on the screen and press the Enter key to save the new calibration settings or press Esc to cancel or quit.

Set the Display Contrast

Adjusting screen contrast lightens or darkens the characters to make them visible at a comfortable level. The contrast is incremented or decremented one step each time the contrast key is pressed.

◐ To adjust screen contrast, locate the <F6> key at the top of the keypad. Adjust the display contrast by pressing the:

- 2nd key then the <F6> key
- Use the Up Arrow and Down Arrow keys to adjust contrast until the display lightens or darkens to your satisfaction.
- Press the Enter key to exit this mode.

The LED for the 2nd key blinks until the special editing mode (set contrast) is complete.

Set the Display Backlight Timer

Note: Refer to the section titled "Power Modes" later in this guide for information relating to the power states of the mobile device.

Select **Start | Settings | Control Panel | Display | Backlight** tab. Change the parameter values and tap OK to save the changes.

The first option affects the mobile device when it is running on battery power only. The second option affects the device when it is running on external power (e.g. AC adapter, cigarette adapter, powered cradle).

The default value for the battery power timer is 3 seconds. The default value for the external power timer is 2 minutes. **The backlight will remain on all the time when both checkboxes are blank.**

The transmissive color display backlight timer *dims the backlight* at the end of the specified time.

Set the Display Brightness

Adjusting screen brightness lightens or darkens the background to make characters visible at a comfortable level. The brightness on a color display is incremented or decremented one step each time the arrow key is pressed until either the maximum or minimum brightness is achieved (8 steps). The brightness setting is recalled at power up.

Locate the <F10> key at the top of the keypad. Adjust the display brightness by pressing the:

- 2nd key then the <F10> key
- Use the Up Arrow and Down Arrow keys to adjust brightness until the display lightens or darkens to your satisfaction.
- Press the Enter key to exit this mode.

The LED for the 2nd key blinks until the special editing mode (set display brightness) is complete.

Set the Power Schemes Timers

Note: Refer to the section titled "Power Modes" later in this guide for information relating to the power states of the mobile device.

Select **Start | Settings | Control Panel | Power | Schemes** tab. Change the parameter values and tap OK to save the changes.

Battery Power Scheme

Use this option when the device will be running on battery power only.

Switch state to User Idle:	Default is After 3 seconds
Switch state to System Idle:	Default is After 15 seconds
Switch state to Suspend:	Default is After 5 minutes

AC Power Scheme

Use this option when the device will be running on external power (e.g. AC adapter, cigarette adapter, powered cradle).

Switch state to User Idle:	Default is After 2 minute
Switch state to System Idle:	Default is After 2 minutes
Switch state to Suspend:	Default is After 5 minutes

These mode timers are cumulative. The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired. When the User Idle timer is set to "Never", the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

Because of the cumulative effect, and using the Battery Power Scheme Defaults listed above:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15sec + 3sec),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.

Set the Audio Speaker Volume

Note: An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.

The speaker is located on the front of the device above the Power button. The audio volume can be adjusted to a comfortable level for the user.

The volume is increased or decreased one step each time the volume key is pressed.

The device has an internal speaker and a jack for an external headset. Operational “beeps” are emitted from the speaker.

Using the Keypad

Note: Volume & Sounds (in Control Panel) must be enabled before the following key sequences will adjust the volume.

◀ To adjust speaker volume, locate the <F8> key at the top of the keypad. Adjust the speaker volume by pressing the:

- 2nd key then the <F8> key to enter Volume change mode.
- Use the Up Arrow and Down Arrow keys to adjust volume until the speaker volume is satisfactory.
- Press the Enter key to exit this mode.

The LED for the 2nd key blinks until the special editing mode (set audio speaker volume) is complete.

Using the Touchscreen

Select **Start | Settings | Control Panel | Volume & Sounds | Volume** tab. Change the volume setting and tap OK to save the change. You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

As the volume scrollbar is moved between Loud and Soft, the computer will emit a tone each time the volume increases or decreases in decibel range.

Setup the Radio and Network

Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys

See “Chapter 4 Wireless Network Configuration” for complete information.

Access the Terminal Emulation Parameters

Before you make a host connection, you will, at a minimum, need to know:

- the alias name or IP address (Host Address) and
- the port number (Telnet Port) of the host system

to properly set up your host session.

1. Make sure the mobile client network settings are configured and functional. If you are connecting over wireless LAN (802.11), make sure your mobile client is communicating with the Access Point.
2. From the **Start | Programs**, run **LXE RFTerm** or tap the **RFTerm** icon on the desktop.
3. Select **Session | Configure** from the application menu and select the “host type” that you require. This will depend on the type of host system that you are going to connect to; i.e. 3270 mainframe, AS/400 5250 server or VT host.
4. Enter the “Host Address” of the host system that you wish to connect to. This may either be a DNS name or an IP address of the host system.
5. Update the telnet port number, if your host application is configured to listen on a specific port. If not, use the default telnet port.
6. Select **OK.**
7. Select **Session | Connect** from the application menu or tap the “Connect” button on the Command Bar. Upon a successful connection, you should see the host application screen displayed.

To change options such as Display, Colors, Cursor, Barcode, etc., please refer to the “RFTerm Reference Guide” on the LXE Manuals CD.

Read an RFID Tag

1. Set RFID tag read parameters using **Start | Settings | Control Panel | RFID**. See Chapter 3 “System Configuration” section titled “RFID”.
2. Set Scanner properties using **Start | Settings | Control Panel | Scanner**.
3. Open the application or text file that is to gather the data read from tags.
4. Place the MX3-RFID within the boundary parameters of the tag to be read. See “RFID Reader Scan Range”.
5. Press the RFID Read button.
6. The data gathered from the tag is sent to the open file.
7. Save the file. The tag read data is ready for further processing.

Note: Control Panel parameters established in Display Properties, Power Properties and Volume & Sounds Properties remain in effect during RFID configuration and the resulting read functions.

Note: Any tag data retrieved and not saved is lost during a reboot or reset.

Installing PCMCIA and CF Cards

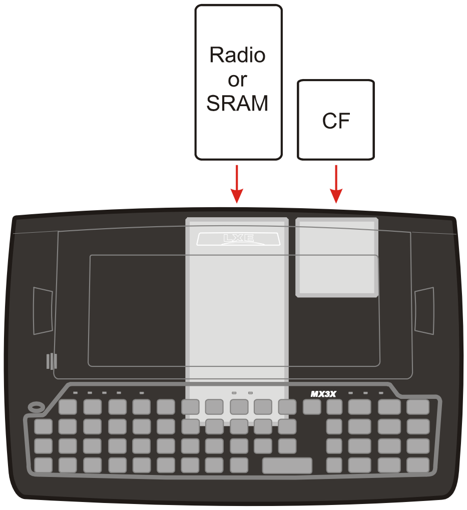


Figure 1-14 PCMCIA and CF Card Location

There is one PC card slot (Slot 0) and one Compact Flash card slot (Slot 1) located under the endcap. Slot 0 powers a radio PC card, PC SRAM card, ATA Flash card or a linear Flash card. The slots hold only one card at a time. Slot 0 supplies .75 of an amp at 5V or 3.3V.

The second slot (Slot 1) is designed to support a Type I or II Compact Flash disk.

See “Chapter 2 Physical Description and Layout”, section titled “PCMCIA Cards” for further information.

Installing / Removing Cards

Preparation

Requirement: A screwdriver (not supplied by LXE)

- LXE recommends that installation or removal of the card be performed on a clean, well-lit surface.
- Using a screwdriver, remove or loosen the screws on the endcap.
- Carefully slide the endcap to the side, taking care not to dislodge or disconnect any cables.
- Remove or loosen all cables to the card(s) to be removed/replaced. If a radio card, disconnect the radio antenna from the radio card.

Installation

1. Slide the card, connector side first, into the slot until it seats. Use caution not to pull or snag the antenna connector.
2. If the card is difficult to seat in the slot, remove the card, turn it around and re-install.
   - The radio antenna connector must be positioned up and toward the front of the device (near the display).
   - Gently snap the antenna cables into the connectors on the radio card. Use caution not to damage either the antenna cable connectors or the connectors on the radio. Connect **all** antenna cables to the PCMCIA radio card.

3. Replace the endcap, making sure all connections are secure and ribbons/antennas are not crimped between the endcap and the body of the mobile device.

Removal

1. Grasp the top of the card and pull it straight upward to remove.
2. Use caution not to pull or snag the antenna connector on the Radio card, if installed.

If you anticipate keeping the PCMCIA or CF card out of the mobile device for a long period of time place it in an enclosed electrostatic-protected storage container. Store in an area that is protected from dirt, moisture, and electrostatic contact.

Entering Data

You can enter data into the mobile device through several different methods. The Scanner window accepts barcode data entry, the RS232 and the IR port are used to input/output data, and the keypad and stylus provide manual entry.

Keypad Entry

The keypad is used to manually input data that is not collected otherwise. Almost any function that a full sized computer keyboard can provide is duplicated on the mobile device's keypad but it may take a few more keystrokes to accomplish a keyed task.

Almost every key has two or three different functions. The primary alpha or numeric character is printed on the key.

For example, when the 2^{nd} key is pressed, the 2^{nd} key LED illuminates. By then pressing the desired second-function key the device will then produce the 2^{nd} character. The specific 2^{nd} character is printed above the corresponding key. The 2^{nd} key LED turns off when key sequence finishes (unless when setting volume or contrast – the 2^{nd} key LED will flash at those times).

Please refer to "Appendix A – Key Maps" for instruction on the specific keypresses to access all keypad functions.

Stylus Entry

The stylus performs the same function as a mouse that is used to point to and click elements on a desktop computer. The stylus is used in the same manner as a mouse – single tap or double tap to select menu options, drag the stylus across text to select, hold the stylus down to activate slider bars, etcetera. Always use the point of the stylus for tapping or making strokes on the display. Never use an actual pen, pencil or sharp or abrasive object to write on the touchscreen.

Hold the stylus as if it were a pen or pencil. Touch an element on the screen with the tip of the stylus then remove the stylus from the screen. The touchscreen responds to an actuation force (touch) of 4 oz. (or greater) of pressure.

The stylus can be used in conjunction with the keyboard and scanner and an input/output device connected to one of the serial ports.

- Touch the stylus to the field of the data entry form to receive the next data feed.
- The cursor begins to flash in the field.
- The unit is ready to accept data from either the keyboard, integrated scanner or a scanner connected to the serial port, if the scanner applet is configured correctly.

Input Panel

The Input Panel icon looks like a keyboard and is shown in the System tray. To show or hide the input panel, tap the Input Panel icon. Use the input panel to enter information in any program.

Integrated Laser Scanner Data Entry

Read all cautions, warnings and labels **before** using the laser scanner.

To scan with the integrated laser barcode reader, point the laser window towards a barcode and press the Scan button. You will see a red laser beam strike the barcode.

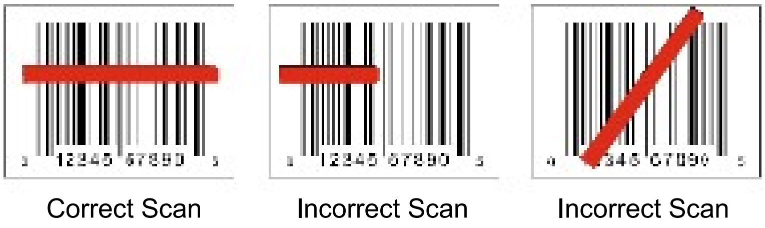

Correct Scan Incorrect Scan Incorrect Scan

Figure 1-15 Scan Beam

Align the red beam so that the barcode is centered within the beam. The laser beam must cross the entire barcode. Move the mobile device towards or away from the barcode so that the barcode takes up approximately two-thirds the width of the beam.

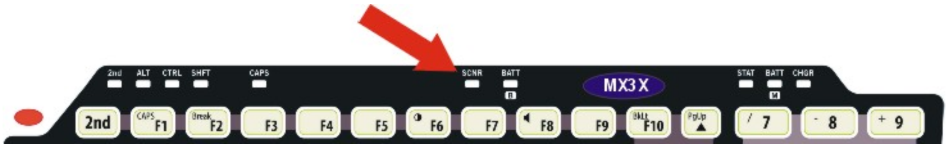


Figure 1-16 Scanner LED Location

The SCNR LED turns red when the laser beam is on. Following a barcode scan and read the SCNR LED turns green and the mobile device beeps, indicating a successful scan.

The laser and SCNR LED automatically turn off after a successful or unsuccessful read. The scanner is ready to scan again when the Scan key is pressed.

Large barcodes can be scanned at the maximum distance. Hold the scanner closer to small barcodes (or with bars that are very close together).

When the scan is successful, the Scan LED turns green, then switches off, and the mobile device emits a distinctive audible tone.

When the scan is unsuccessful, the SCNR LED remains red until the 3 second timeout (default) occurs or the Scan key is released. The mobile device emits distinctive audible tones. Check the following:

- Check the barcode for marks or physical damage e.g. ripped label, missing section, etc.
- Try scanning test symbols of the same code type at different distances and angles.
- Is the scan aperture unscratched and unsoiled?

Note: An MX3-RFID manufactured prior to July 2006 contained an SE923 barcode scanner. The SE955 scanner replaced the SE923 scanner in devices manufactured after July 2006.

See the "Integrated Scanner Programming Guide" for scanner engine programming barcodes, default scanning ranges, barcode reading instruction and troubleshooting.

RFID Tag Data Collection

When the RFID Read button is pressed, the reader turns on and the MX3-RFID beeps once if the tag was located and read successfully. The reader turns off at a predetermined time limit after a good read or a failed read.

There may be a buzz sound during the time the reader is "searching and reading" if the RFID reader is configured to buzz during a read cycle.

See Chapter 3 "System Configuration" section titled "RFID".

Tethered Scanner

Tethered scanners connected to an RS232 port are not supported on the MX3-RFID.

Do ***not*** *connect a tethered scanner cable to a USB-C or USB-H labeled endcap port. They are USB ports and cannot power a tethered scanner*.

ActiveSync

Introduction

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the radio link, serial port, USB or the infrared port on the mobile device.

Requirement: ActiveSync version 3.7 (or higher) must be resident on the host (desktop/laptop) computer. ActiveSync is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync on your desktop computer.

Using Microsoft ActiveSync version 3.7 or higher, you can synchronize information on your desktop computer with the mobile device and vice versa. Synchronization compares the data on your mobile device with your desktop computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.

By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your desktop computer and your device.

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your device to your desktop computer,
- set up a partnership so you can synchronize information between your device and your desktop computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard. For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The following instructions relate to the initial setup of ActiveSync. When there is a Connect icon on the desktop, this section can be bypassed.

The partnerships can only be created using direct serial or USB cable connection. After the partnerships are established, ActiveSync communication can be initiated using serial, USB, IrDa and radio. See section titled "Connect and Communicate" for cable/port compatibility.

USB Connection

Select **Start | Settings | Control Panel | PC Connection**. Tap the Change button. From the popup list, choose

USB "Client"

This will set up the mobile device to use the USB port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel.

IMPORTANT – DO NOT PUT THE MOBILE DEVICE INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

The MX3-RFID requires USB connection for ActiveSync. There is no ActiveSync connection through the MX3-RFID passive cradle.

Serial Connection

Select **Start | Settings | Control Panel | PC Connection**. Tap the Change button. From the popup list, choose

Serial 1 @ 57600

Note: The default is 57600 baud.

This will set up the mobile device to use COM 1. If the device has a dual-serial port endcap, the Serial 3 @ 57600 can also be selected. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel.

Select Scanner and ensure the integrated scanner is set to a port that is NOT the same as the ActiveSync port.

Radio

Note: You must establish a partnership with a desktop computer prior to running ActiveSync on the mobile device. The initial partnership must be done using direct serial / USB cable connection.

Once the relationship is established using the serial port, the ActiveSync link in the Start Menu gives a choice of connections, one of which is radio.

Select **Start | Settings | Programs | Communication | ActiveSync**. From the popup list, choose Network and then tap the Connect button.

IrDA Connection

Note: The ActiveSync connection does true IrDA, not serial over IR, or TCP/IP (Winsock) over IR, like many infrared connections. Therefore, it is important to use a PC infrared interface which supports the handshaking needed for ActiveSync. This, unfortunately, precludes using many brands of laptops, which only use a simple infrared interface, even though they may call it IrDA.

Select **Start | Settings | Control Panel | PC Connection**. Tap the Change button. From the popup list, choose

IR @ 115200

This will set up the mobile device to use the Infrared port. Tap OK and ensure the check box for “Allow connection with desktop computer when device is attached” is checked.

Tap OK to return to the Control Panel.

Select Scanner and ensure the integrated scanner is set to a port that is NOT the same as the ActiveSync port.

Synchronizing from the Mobile Device

To synchronize using a wireless LAN card, you must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device (see “Initial Setup”).

To initiate synchronization from your device, tap **Start | Programs | Communication | ActiveSync** to begin the process.

Tap **Sync** to connect and synchronize. View synchronization status.

Tap **Tools** to synchronize or change synchronization settings. View connection status.

Tap **Stop** to stop synchronization.

Tap **Start | Help** for context-sensitive help.

Connect and Communicate

Connect the correct** cable to the PC (the host) and the mobile device (the client). Select "Connect" from the Start Menu on the client (**Start | Programs | Communications | Connect**).

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Note: USB will start automatically when the USB cable is connected, not requiring you to select "Connect" from the start menu.

** Cable for initial ActiveSync Configuration:

USB Client to PC/Laptop	USB-Client cable	MX3XA069CBLD9USBCLNT

Explore

From the ActiveSync Dialog on the Desktop PC, tap the Explore button, which allows you to explore the mobile device from the PC side, with some limitations. You can copy files to or from the mobile device by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the mobile device. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows CE .NET image. This, however, includes most of the files in the \Windows folder).

Copy the MX3-RFID LXEbook to the Mobile Device (Optional)

Note: The LXEbook user guides do not contain the illustrations and regulatory information contained in the full user guides on the LXE Manuals CD and on the LXE ServicePass website. See the full format User Guide"MX3-RFID User's Guide" on LXE Manuals CD.

Mobile Device	Required Adobe Acrobat Reader Version
MX3-RFID	Windows CE. NET PDF Viewer (pre-installed by LXE).

First, using your desktop computer download "LXEbook – MX3-RFID Users Guide" from the LXE Manuals CD to your desktop computer.

Next, connect the mobile device to your desktop computer and run ActiveSync.

When the mobile device and the desktop ActiveSync applications are synchronized, click Explore on the ActiveSync menu on your desktop to display the contents of the mobile device folders.

Then, open the folder on your desktop computer containing the downloaded LXEbook User's Guide. Click and drag the LXEbook User Guide to the My Documents folder on the mobile device.

When the file copy process is finished, disconnect the mobile device from the synchronization equipment and close ActiveSync.

To view the LXEbook on the mobile device, select Start / Programs / Adobe Reader / File / Open. Locate the LXEbook on the mobile device and "open" the file.

See Also: "Install LXEbooks" on the LXE Manuals CD.

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a desktop or laptop PC using the appropriate cable and Microsoft's ActiveSync.

Prerequisites

A partnership between the mobile device and ActiveSync has been established. See section titled "Initial Setup".

Serial Port Transfer

- A desktop or laptop PC with an available serial port and a mobile device with a serial port. The desktop or laptop PC must be running Windows 2000 or greater.
- Null modem cable with all control lines connected. LXE recommends using the null modem cable part number listed in "Accessories".

Infrared Port Transfer

- A desktop or laptop PC with an infrared port and a mobile device with an infrared port. The desktop or laptop PC must be running Windows 2000 or greater.

USB Transfer

- A desktop or laptop PC with an available USB port and a mobile device with a USB port. The desktop or laptop PC must be running Windows 2000 or greater.
- Use the MX3-RFID-specific USB cable as listed in "Accessories".

Connect

Connect the USB cable to the PC (the host) and the mobile device (the client). USB synchronization will start automatically when the cable is connected. If needed, select "Connect" from the Start Menu on the mobile device (**Start | Programs | Communications | Connect)**.

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Disconnect

Serial Connection

- Disconnect the cable from the mobile device.
- Put the mobile device into suspend by tapping the red Suspend button.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

IRDA Connection

- Move the mobile device so the infrared beam is broken.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

USB Connection

- Disconnect the cable from the mobile device.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

IMPORTANT – Do not put the mobile device into suspend while connected via USB. The device will be unable to connect to the host PC when it resumes operation.

Radio Connection

- Put the mobile device into suspend by tapping the red Suspend button.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

When the mobile device is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (**Control Panel | System | Device Name**)

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy *that* partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

Troubleshooting ActiveSync

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

If the MX3-RFID is connected to a PC by the USB cable, disconnect the cable from the mobile device and connect it again.

Check that the correct connection is selected (Serial or USB "Client" if this is the initial ActiveSync installation).

See Also: "Cold Boot and Loss of Host Reconnection".

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon (or REPLLOG.EXE in the Windows directory).

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

ActiveSync indicator on the host turns green and spins, but connection never occurs

Baud rate of connection is not supported or detected by host. Check that the correct connection is selected (Serial or USB "Client" if this is the initial ActiveSync installation).

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

The host doesn't know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Testing connection with a terminal emulator program, or a serial port monitor

You can use HyperTerminal or some other terminal emulator program to do a rough test of ActiveSync. Set the terminal emulator to 8 bits, no parity, 1 stop bits, and the same baud rate as the connection on the CE device. After double-tapping REPLLOG.EXE on the CE device, the word "CLIENT" appears on the display in ASCII format. When using a serial port monitor, you see the host echo "CLIENT", followed by "SERVER". After this point, the data stream becomes straight (binary) PPP.

The Passive Vehicle Cradle

The MX3-RFID cannot fit in standard MX3 charging cradles. The passive vehicle mount cradle is designed for the MX3-RFID. The passive vehicle cradle does not have LEDs or indicators. The passive vehicle cradle does not require an external power source.

The MX3-RFID seated in the passive cradle requires a power source, either from the main battery or from power applied via the power jack on the endcap. The MX3-RFID requires USB connection for ActiveSync. There is no ActiveSync connection through the MX3-RFID passive cradle, only through the USB port on the MX3-RFID endcap.

The cradle restrains the mobile device. The cradle is designed to be securely mounted to a vehicle. The passive cradle does not have external device connectors e.g. power/serial cable. Power can be applied to the mobile device through the power jack in the endcap only. Wireless client interaction is available as long as the mobile device has sufficient energy in the main battery pack and a clear signal path.

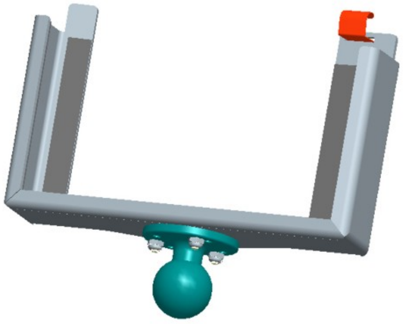


Figure 1-17 MX3-RFID Passive Cradle with Attached RAM Ball

The cradle is lined with strips of hook-and-loop fabric to ensure a snug fit between the mobile device and the inside of the cradle. A thumb-spring at the top of the cradle secures the mobile device in the cradle. Hold the thumb spring up and slide the device into the cradle, release the thumb spring and it will click in place. The mobile device is removed from the cradle by pressing the thumb spring up and then grasping the mobile device and pulling it straight up and away from the cradle.

The vehicle cradle should be mounted in an area in the vehicle where it:

- Does not obstruct the driver's vision or safe vehicle operation.
- Will be protected from rain or inclement weather.
- Will be protected from extremely high concentrations of dust or wind-blown debris.
- Can be easily accessed by a user seated in the driver's seat.

A RAM ball cylinder mounting option is used to secure the cradle to the vehicle. A RAM ball may be pre-installed to the cradle by LXE.

Check the cradle regularly for excessive wear at pressure points. If the cradle becomes cracked or broken at any time, it must be taken out of service and replaced. Contact LXE Customer Service for a replacement MX3-RFID passive cradle (see "Getting Help").

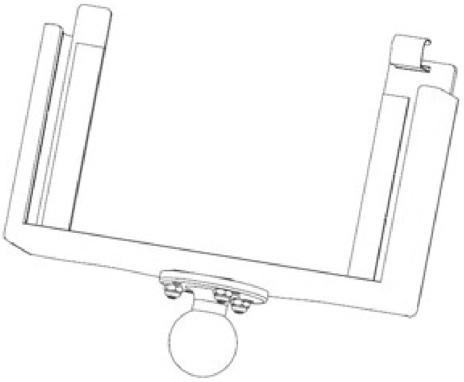
Before installation begins, verify you have the applicable vehicle mounting RAM ball assembly components necessary for your mount type, as shown in the section titled “Passive Cradle Assembly Components”.

Do not slide the mobile device into the passive cradle until the cradle is securely fastened to the vehicle.

Passive Cradle Assembly Components

Note: LXE does not supply the bolts or washers needed when mounting the RAM ball to the vehicle chassis. LXE recommends using bolts with a maximum 10/32” (0.3125) diameter.

Passive Cradle



RAM Ball and Arm Cylinder

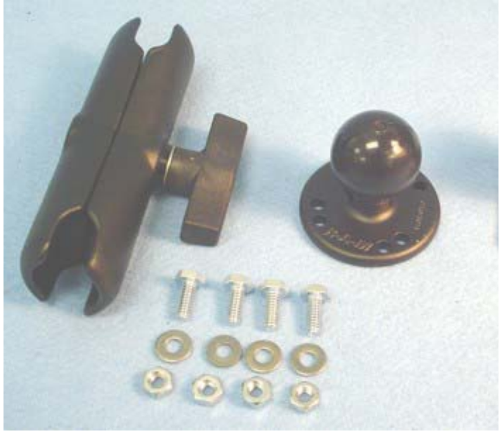
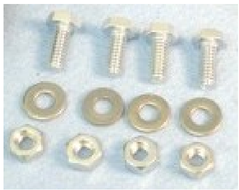
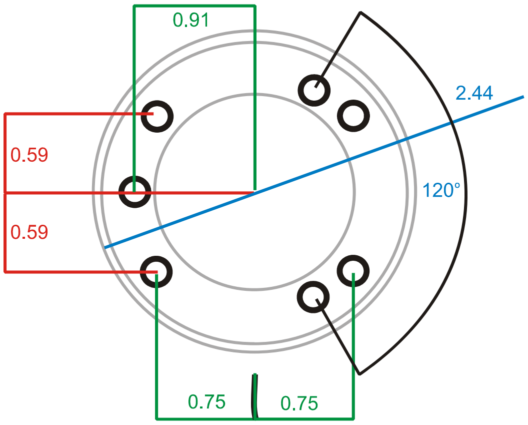
	 Qty 4 - Hex Cap 1/4-20 x 3/4 bolts Qty 4 - 1/4 flat washer Qty 4 - 1/4-20 nylon insert lock nuts

Figure 1-18 RAM Bracket Kit Components

Mount the RAM ball to the bottom of the cradle with the bolts, washers and nuts supplied by LXE.

RAM Mount Assembly



Not To Scale

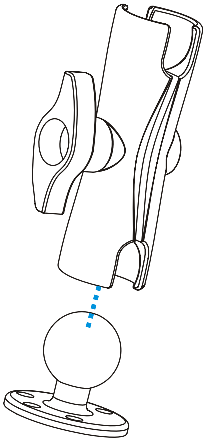
Figure 1-19 RAM Assembly Footprint

Note: LXE does not supply the bolts or washers needed when mounting the RAM ball to the vehicle chassis. LXE recommends using bolts with a maximum 10/32" (0.3125) diameter.

1. Attach the RAM ball to the vehicle, making sure it does not impede safe operation of the vehicle.

2. If necessary, fasten the upper RAM ball assembly to the base of the passive cradle using the supplied bolts, washers and screws.

3. Loosen the turnscrew on the RAM arm, place the lower socket over the vehicle mounted RAM ball, then the other arm socket over the RAM ball mounted to the cradle.



4. Tighten the arm turnscrew until the cradle is secured to the RAM arm and the vehicle.

5. The MX3-RFID passive vehicle mounted cradle is ready for use.

Getting Help

All LXE user guides are now available on one CD and they can also be viewed/downloaded from the LXE ServicePass website. Contact your LXE representative to obtain the LXE Manuals CD.

You can also get help from LXE by calling the telephone numbers listed on the LXE Manuals CD, in the file titled "Contacting LXE". This information is also available on the LXE website.

Explanations of terms and acronyms used in this guide are located in the file titled "LXE Technical Glossary" on the LXE Manuals CD.

Manuals

MX3-RFID User’s Guide
LXEbook – MX3-RFID User’s Guide (download to mobile device)
MX3 Cradle Reference Guide
MX3 Multi-Charger Plus User’s Guide
CE API Programming Guide
RFTerm Reference Guide
Integrated Scanner Reference Guide

Accessories

Battery Charger/Analyzer, US V1.01	9000A377CHGR5US
AC Power Cable, US	9000A066CBLPWRAC
Battery, Replacement, RFID Device	MX3A380RFIDBATT
AC Power Supply, US	9000A301PSACUS
Power Supply, Cigarette Lighter Adapter	9000A303PSCIGLTADPT
MX3-RFID Nylon Case with Shoulder Strap	MX3XA411RFIDCASE
MX3-RFID Passive Mounting Cradle	MX3XA001RFIDCRADLE
RAM Mount Kit	9000A019RAMKIT
Cable, USB Client D95 to USB Client Device Type A Plug, 6 ft – for USB ActiveSync	MX3XA069CBLD9USBCLNT
Stylus Kit includes stick-on clip, stylus and tether (5 pack)	9000A507STYLUS
Stylus Kit includes stick-on clip, stylus and tether (1 pack)	9000A501PASSIVEPEN
CD with CE .NET and LXE API’s and documentation for custom application development with RFID functions	MX3XA504CENET42SDK
Touchscreen Protective Film, Color Display (10 pack)	MX3XA503PROTFILMCOLR

Note: MX3-RFID mobile devices are available in the US only.

Chapter 2 Physical Description and Layout

Hardware Configuration

The MX3-RFID hardware configuration is shown in the following figure.

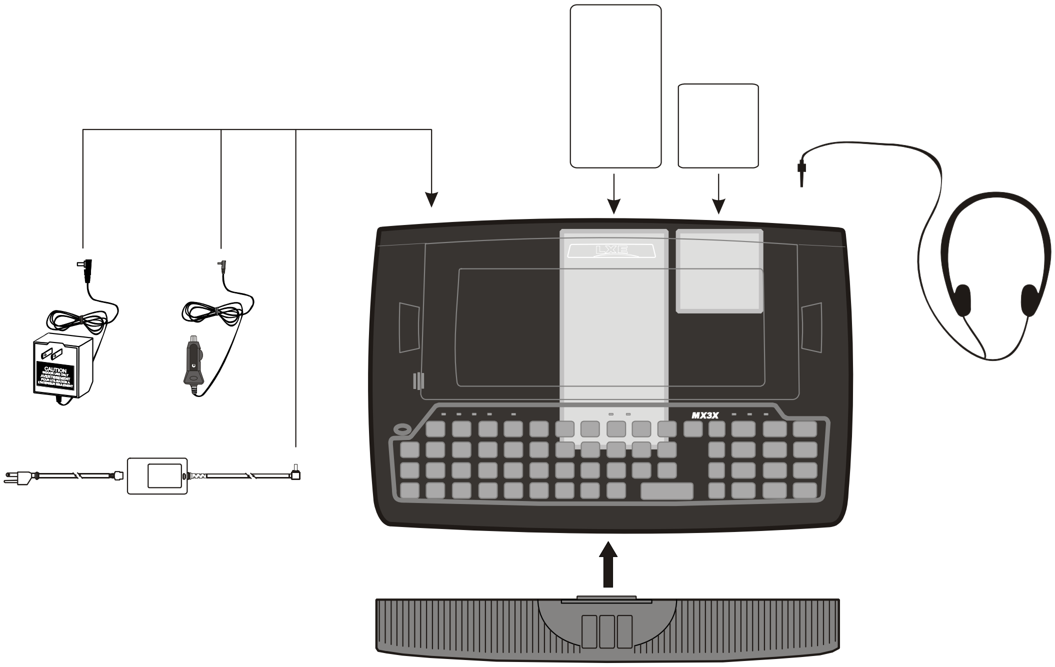


Figure 2-1 Hardware

Central Processing Unit

The CPU is an Intel Xscale PXA255 running at 400 MHz.

System Memory

A CF Card FLASH is used for ROM, Flash for Windows CE .NET and Flash memory for bundled applications. The Flash is configured as the primary boot device and contains the Windows CE .NET image, boot loader, OAL, applications, utilities and device drivers.

Any flash remaining beyond the Windows CE .NET image is formatted for use as a persistent memory drive (which appears in My Computer as the folder “System”). Any programs or data stored in this folder will not be lost if the memory backup battery fails.

The computer has one Type II CF+ slot. The computer supports and auto detects up to 256MB of Type I compact flash memory.

Core Logic

The mobile device supports the following I/O components of the core logic:

- One PCMCIA slot (supports Type I or II PCMCIA cards). The Summit Client device is in a PCMCIA Adapter card in this slot.
- One compact Flash card port (supports Type I and II cards).
- One InfraRed port.
- One Digitizer Input port (see section titled "Touchscreen").
- Two I/O ports in six configurations (see section titled "Endcaps and COM Ports.").

Video Subsystem

The display has a 640 pixel (horizontal) by 240 pixel (vertical) format. The display contrast is adjustable with key sequences. Backlighting is available and can be adjusted with key sequences. The turn-off timing is configured through the Control Panel. The display controller supports Windows CE graphics modes. Touchscreen allows mouse functions (pointing and taping on the display or Signature Capture) using an LXE approved stylus.

There are two types of displays available: transflective greyscale monochrome; and transmissive color. The transmissive color display is optimized for indoor lighting. It cannot be used without the backlight. The transflective monochrome is optimized for outdoor use but may also be used indoors. The monochrome display has an electroluminescent backlight. The color displays have a CCFL (Cold-Cathode Fluorescent Lighting) backlight.

The transflective display appears to have a greenish hue when the display is off or suspended. The transmissive display appears black when the display is off or suspended.

See Section "Display" .

Power Supply

The mobile device uses two batteries for operation.

- An 1900 mAh replaceable Lithium-Ion (Li-Ion) battery pack. The battery pack recharges while the computer is in a powered cradle or when connected to the optional external power sources. The main battery can be removed and inserted in the MX3 Multi-Charger which simultaneously charges up to six battery packs in four hours.
- An internal 50 mAh Nickel Cadmium (NiCd) backup battery. The backup battery is recharged directly by the main battery when it is in the mobile device. Full charging of the backup battery may take several hours. The recharging of the backup battery is automatically controlled by the operating system. The backup battery must be replaced by qualified service personnel.

Optional AC adapters are available – external AC power supplies (US and International) and a cigarette lighter adapter. See Chapter 3 "Power Supply", "External Power Supply".

When the backup battery and main battery are dead, the mobile device reverts to it's default values when a fully charged main battery is installed and the device is powered On again. Follow the steps in section titled "Getting Started".

Audio Interface

An interface is available for headset operation. When a headset is plugged into the audio jack on the endcap, the main speaker is disabled.

PCMCIA Slots

Use and operation of the Personal Computer Memory Card International Association (PCMCIA) device (e.g. PC card) is dependent upon both the type of device installed and the application(s) running on the computer.

Make sure the proper software is pre-loaded and PC cards are properly configured.

Slot 0 – Radio or SRAM Cards

Note: When removing or installing the radio, protect the internal components and the radio from electrostatic discharge.

The mobile device has one internal PCMCIA slot that conforms electrically to PCMCIA 2.1 specifications. The PC Slot supplies 0.75 of an amp at 5Volts or 3.3Volts. Battery voltage is supplied through unused pin 35 to support a WAN radio in the slot.

The PC slot is accessible by the use of a Phillips screwdriver to first loosen the endcap. It accepts Type I or II cards only. Slot 0 accepts PCMCIA 2.4GHz radio cards or SRAM/Flash memory cards.

Slot 1 – Compact Flash Card

The mobile device has one internal Compact Flash card port that supports Type I and II CF+ cards. The slot is accessible when the endcap has been loosened.

RFID Reader Scan Range

Type of Tag	Scan Range
Class 0 Tag	2 feet / .7 meters
Class 1 Tag	3 feet / .9 meters
Class 1 Gen 2 Tag	1 foot / .3 meters

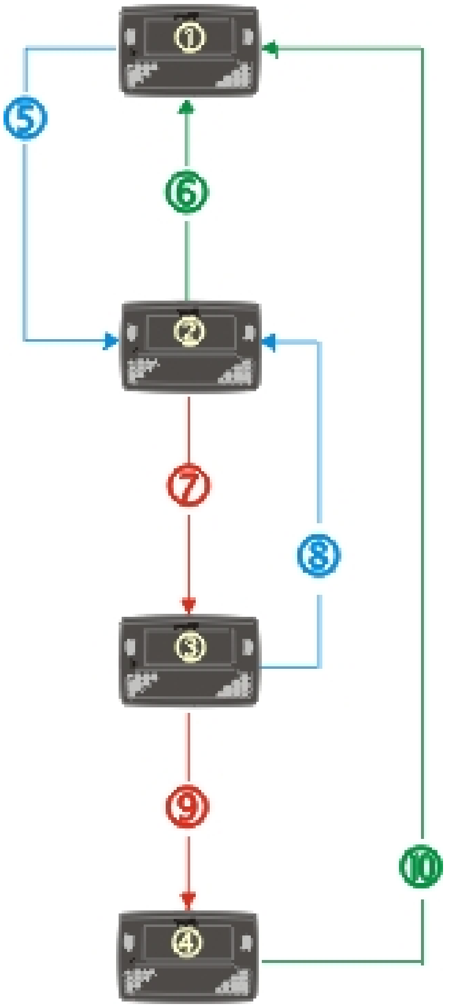
Figure 2-2 RFID Tag Reading Ranges

Unlike barcode scanners that require line-of-sight before successfully reading a barcode, the RFID reader does not require line-of-sight when searching for and reading tags. Pressing the RFID Read button on the MX3-RFID starts a 360 degree search "beam" that stops at the limits of the scan range of the RFID reader. The "beam" stops searching when the read timer expires.

The integrated laser barcode scanner can only read barcodes. The MX3-RFID cannot read barcode labels and RFID labels at the same time. For example, the MX3-RFID can scan a barcode label and when the good read/bad read/store data process is complete, it is then free to begin the process of reading and storing the data from an RFID tag.

The RFID module can only read RFID tags.

Power Modes



1 – **On**

2 – **Suspend**

3 – **Critical Suspend**

4 – **Off**

5 – Power Button or Power Off Timer expires

6 – Primary Event

7 – Power fail. Also from Suspend (2) or On (1).

8 – Restoration of power.

9 – Backup battery and main battery dead

10 – Power applied. New main battery installed or external power applied. Tap the Power button.

Note: After event 8, the only primary event (6) which functions is a power button tap.

Figure 2-3 Power Modes – On, Suspend, Critical Suspend and Off

Primary Events Listing

Any key on the keypad	COM1 activity
Stylus touch on the touchscreen	COM2 activity
Power button tap	COM3 activity
PC card activity	USB client connection
External power connection	Scanner activity

On Mode

The Display

When the display is On:

- the keyboard, touchscreen and all peripherals function normally
- the display backlight is on until the Backlight timer expires (default is 3 seconds) 15 seconds afterwards, the display turns off.
- when the main battery is hot-swapped, the display is turned Off.

The Mobile Device

After a new mobile device has been received, a charged main battery inserted, and the Power button tapped, the computer is always On until both batteries are drained completely of power.

When the main battery and backup battery are drained completely, the unit is in the Off mode. The unit transitions from the Off mode to the On mode when a charged main battery is inserted or external power is applied. Press the Power button to turn the device on.

User Idle Mode

Note: When the display backlight is Off, the unit is still On. The unit functions normally – a tethered scanner trigger press or an integrated scanner Scan key press will cause scans. Communications through the radio or serial ports continue.

User Idle timers are set using **Start | Settings | Control Panel | Power | Schemes** tab.

The display backlight is turned off when one of the following occurs:

- the user idle timer expires before a wakeup event takes place
- the Power button is tapped which immediately places the unit into Suspend Mode.

Display Backlight Suspend timers are set using **Start | Settings | Control Panel | Display | Backlight** tab.

Any of the following primary events will wake the display and display backlight:

Any key on the keypad
Stylus touch on the touchscreen
Power button tap

When the display backlight wakes up, the User Idle Timer begins the countdown again. When any of the above events occur prior to the timer expiring, the timer begins the countdown again.

The first display backlight wakeup key press or touch is sent to the operating system or running application. Once the display is On, the keyboard and touchscreen function normally.

System Idle Mode

Note: When the display is Off, the unit is still On. The unit functions normally – tethered scanner trigger press or integrated scanner Scan key press will cause scans. Communications through the radio or serial ports continue.

System Idle timers are set using **Start | Settings | Control Panel | Power | Schemes** tab.

The display is turned off when the System Idle timer expires before a wakeup event takes place.

The Power button is tapped which immediately wakes the unit up.

The Status LED blinks green when the Display enters Off mode.

Any of the following primary events will wake the display and display backlight:

Any key on the keypad
Stylus touch on the touchscreen
Power button tap

When the display wakes up, the System Idle Timer begins the countdown again. When any of the above events occur prior to the timer expiring, the timer begins the countdown again.

The first display wakeup key press or touch is sent to the operating system or running application. Once the display is On, the keyboard and touchscreen function normally.

Suspend Mode

The Suspend mode is entered when the device is either inactive for a predetermined period of time, the user taps the Power button or the user selects **Start | Suspend**.

Suspend timers are set using **Start | Settings | Control Panel | Power | Schemes** tab.

Any of the following can be configured to wake the unit and reset both the display and display backlight timers:

Any key on the keypad	PC card activity
Power button tap	Stylus touch on the touchscreen
COM1 CTS	External power connection
COM3 CTS	USB client connection

When the device wakes up, the User Idle, System Idle and the Suspend timers begin the countdown again. When any one of the above events occurs prior to the Suspend timer expiring, the timer starts the countdown again.

The first wakeup key press or touch is not sent to the operating system or running application – the first keypress or touch is only used to wake up the unit and reset the timers. Once the unit has transitioned from the Suspend mode to the On mode, the unit, keyboard and touchscreen function normally.

Critical Suspend Mode

The purpose of the Critical Suspend mode is to reduce power consumption to a lower level that still retains the contents of SDRAM. The device enters Critical Suspend Mode only when the main battery has failed or is removed/hot-swapped. The backup battery is supplying power to the unit during Critical Suspend Mode.

When hot-swapping (the main battery is removed and replaced), the display turns off, the BATT M LED begins to flash red, all peripherals are shut down, the CPU clock is stopped, and power is removed from the PCMCIA card.

When the device is in the Critical Suspend state (the main battery is in place and the device is being powered by the backup battery), the display turns off, the BATT M LED begins to flash red, all peripherals are shut down, the CPU clock is stopped, and power is removed from the PCMCIA card. The operating system is saving the state prior to the main battery failing and cannot be used.

If a fully charged main battery is installed before the backup battery is depleted (approximately 5 minutes) the device transitions to the Suspend state. To resume operation tap the Power key.

If the backup battery is depleted before a fully charged main battery is inserted, the device immediately turns itself Off and all unsaved information is lost. Insert a fully charged main battery and press the Power button to turn the device On.

Off Mode

The unit is in Off Mode when the main battery and the backup battery are depleted.

Insert a fully charged main battery and press the Power button to turn the device On. The mobile device reverts to the last saved default (factory) values. Follow the steps in “Getting Started”.

Physical Controls

Power Button

Note: Refer to the section titled "Power Modes" for information relating to the power states of the mobile device.

The power button is located above the ESC key on the keypad. When a battery is inserted for the first time, the Power button must be pressed.

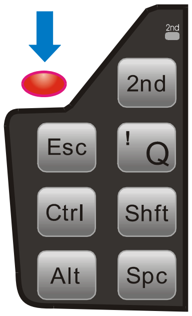


Figure 2-4 Location of the Power (PWR) Button

Quickly tapping the Power button places the device immediately in Suspend mode. Quickly tapping the Power button again, or touching the screen, immediately returns the device from Suspend.

Restart Sequence

Tap **Start | Run,** then type **warmboot** in the textbox and press **Enter.** If the touchscreen is not accepting taps or needs recalibration, press <Ctrl>+<Esc> to force the Start Menu to appear.

When the Windows desktop is displayed or an application begins, the power on (or reboot) sequence is complete. If any changes to the settings had been saved previously, they are restored on reboot.

Any RFID tag data retrieved and not saved is lost during a reboot or reset.

Note: To reset to factory default values, please refer to Chapter 3 "System Configuration" section titled "Utilities".

Endcaps and COM Ports

The MX3-RFID supports three COM port options. Two external serial ports are dependent on the end cap chosen. A third serial port is used to support an integrated infrared transciever (barcode reader). An additional endcap configuration supports serial and USB “slave” input/output at 1.5 MBps.

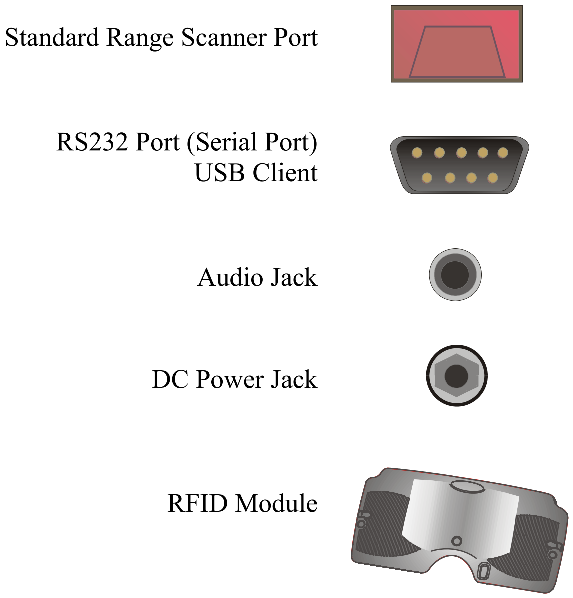


Figure 2-5 Endcap and COM Ports

The COM 2 port is always the IR port on the back of the mobile device, regardless of the type of endcap installed.

On the Standard Range Scanner / Serial Port endcap COM 3 is the Integrated Scanner port. The integrated barcode scanner scans only when the Scan button is pressed. To edit Scanner Com Port parameters, select **Start | Settings | Control Panel | Scanner**. Change the parameter values and tap OK to save the changes.

On the Dual Serial Port endcap the COM1 port is the serial port on the right side of the endcap when the display is facing you.

Endcap Combination

Left Port	Right Port
Laser Scanner	USB Client

With the screen facing up, specifically, the assignment of the serial ports is as follows:

- COM1 for the RFID module.
- COM 2 is always the IR port on the back of the device, regardless of the type of endcap installed.
- COM 3 for either the integrated barcode scanner or an RS232 port.

Integrated Scanner Port

The integrated laser barcode scanner is used to collect barcode data from any nearby compatible barcode label. Depending on the size of the barcode, size of bars and spacing and quality of the barcode, the scanner is used to read barcodes between 3" and 30". The barcode scanner reads UPC/EAN, Code 39, Code 93, I 2 of 5, Discrete 2 of 5, Code 128, Codabar and MSI symbologies.

The integrated laser scanner scans only when the Scan button is pressed. The SCNR LED illuminates during any mobile device integrated scanner activation.

If you need to set up the integrated scanner **barcode reading parameters**, please refer to the "Integrated Scanner Programming Guide" and the "MX3" barcode scanner type. The guide is on the LXE Manuals CD and the LXE ServicePass website.

Note: An MX3-RFID manufactured prior to July 2006 contained an SE923 barcode scanner. The SE955 scanner replaced the SE923 scanner in devices manufactured after July 2006. The "Integrated Scanner Programming Guide" contains both types for scanner engine programming barcodes, default scanning ranges, barcode reading instruction and troubleshooting.

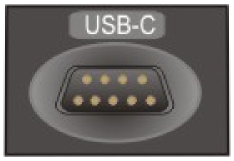
USB Client Port

USB Client connection is made through the USB Port. The connector is an industry-standard 9-pin "D" male connector.

The LXE USB cable is required to adapt the connection to a standard USB connector.

USB Client Cable

MX3XA069CBLD9USBCLNT



Port Label on Endcap

Mobile Device End	Goes To	USB Type A Plug End
1 Host Detect		1
2 Not Used		
3 D + (Green Wire)		3
4 Not Used		
5 Ground (Black Wire)		4
6 Not Used		
7 D – (White Wire)		2
8 Not Used		
9 Not Used		

Figure 2-6 USB Type A to Serial Port Cable Pinout

ActiveSync

Connect from USB-C port to USB Type A Host – a laptop/desktop, etc.

Programmable Scan Buttons

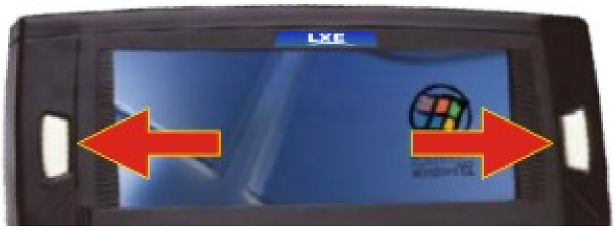


Figure 2-7 Programmable Buttons

There are two buttons, one on each side of the display. The buttons can be programmed to perform specific functions. The programmable keys have no effect on barcode scanners tethered to the device. When there is no integrated scanner installed, both buttons default to Enter buttons (with the exception of IBM 5250 terminal emulation devices – in this case, the left button is labelled and functions as “Field Exit”).

Note: The programmable Scan key can be programmed as the RFID Read key for an MX3-RFID device.

To edit the button parameters, select **Start | Settings | Control Panel | Scanner**. Change the parameter values and tap OK to save the changes.

The default setting for the right button is RFID Read. The default setting for the left button is Scan. When the device does *not* have an integrated scanner, both buttons default to Enter keys and the Scan selection is greyed out.

Each button can be setup as:

- Disabled – no response when pressed
- Scan – initiate a barcode scan sequence (integrated scanner only)
- Enter Key
- Tab Key
- Field Exit (IBM 5250 / TN5250 devices only)
- Virtual Key (default values F20 and F21)
- RFID Read

Field Exit Key Function (IBM 5250/TN5250 Only)

Fld Exit

The Field Exit key is used to exit an input field. If the field is an Auto Enter field, the auto transmit function is activated. This key function is present on the IBM 5250/TN5250 specific keypad only.

Scan Buttons and the SCNR LED

The SCNR LED, located above the keypad, illuminates during an integrated barcode scanner function. It is affected by internal scanner algorithms.

- Red – scanning.
- Green – good scan.
- Unlit – laser scanner is inactive.

The Keypad

The QWERTY keypad is phosphorescent. A phosphorescent keypad does not use a keypad backlight but glows in dim/dark areas after exposure to a light source. The keypad is installed and configured by LXE.

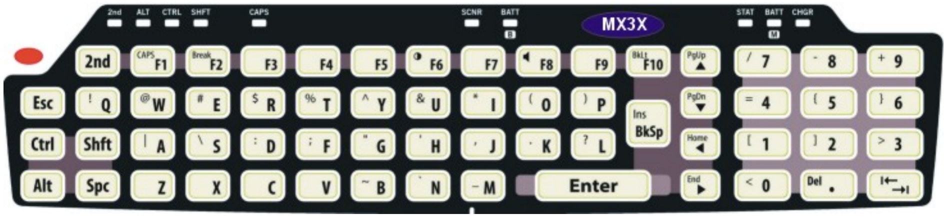


Figure 2-8 The QWERTY Keypad

The keymaps (keypress sequences) are located in “Appendix A – Key Maps.”

Key Functions

Key	Function
Scan	(***Scanner integrated into endcaps only***.) The Scan key activates the scanner when a scanner endcap is installed and the Scan button is pressed. The internal scanner scans only when the Scan button is pressed. A Scan button press has no effect on externally attached scanners. See previous section titled “Programmable Buttons.” When there is no integrated scanner endcap, the Scan keys function as Enter keys. For IBM 5250 configurations, the left button is the “Field Exit” key.
Enter	The Enter key is used to confirm a forms entry or to transmit information. How it is used is determined by the application running on the computer.
2nd	The 2nd key is used to activate the 2nd functions of the keypad. Printed on many keys at the upper left corner are small characters that represent the 2nd function of that key. Using the 2nd key activates the second key function. Note that the 2nd key only stays active for one keystroke. Each time you need to use the 2nd function you must press the 2nd key. To cancel a 2nd function before pressing another key, press the 2nd key again. When the 2nd function is active, the 2nd LED illuminates.
Ctrl	The Ctrl key enables the control functions of the keypad. This function is similar to a regular keyboard’s Control key. Note that the Ctrl key only stays active for one keystroke. Each time you need to use a Ctrl function, you need to press the Ctrl key before pressing the desired key. When the Ctrl function is active, the Ctrl LED illuminates.

Key	Function
Alt	The Alt key enables the alternate functions of the keypad. This function is similar to a regular keyboard's Alt key. Note that the Alt key only stays active for one keystroke. Each time you need to use an alternate function, you need to press the Alt key before pressing the desired key. When the Alt function is active, the Alt LED illuminates.
Shft	The Shft key enables the shifted functions of the keypad. This function is similar to a regular keyboard's Shift key. Note that the Shift key only stays active for one keystroke. Each time you need to use a Shifted function, you need to press the Shft key before pressing the desired key. When the Shft function is active, the Shft LED illuminates. When the Shft key is pressed the next key is determined by the major key legends, i.e., the alpha keys display lower case letters – when CAPS is On alpha characters are capitalized. For example, when CAPS is on and the Shft key and the G key are pressed, a lower case g is displayed.
Spc	The Spc key adds a space to the line of data on the display. This function is similar to a regular keyboard's Spacebar. Note that the Spc key only stays active for one keystroke.

Caps Key and CapsLock Mode

This function is similar to a regular keyboard's CapsLock key. Note that the CapsLock mode stays active until the CapsLock key sequence is pressed again. Each time you need to use a Caps function, you need to press the Caps key sequence first. To cancel a CapsLock function press the Caps key sequence again. When the CapsLock mode is active, the Caps LED illuminates.

The CapsLock key sequence is 2nd + F1.

- No CapsLock AND No Shift keypress – result is a lowercase letter.
- CapsLock OR Shift – result is an uppercase letter.
- CapsLock AND Shift keypress – result is a lowercase letter.

Keypad Shortcuts

Use keyboard shortcuts instead of the stylus:

- Press Tab and an Arrow key to select a file.
- Press Shift and an Arrow key to select several files.
- Once you've selected a file, press Alt then press Enter to open its Properties dialog.
- Press 2nd then press numeric dot to delete a file.
- To force the Start menu to display, press Ctrl then press Esc.

Keypress Sequences

See Appendix A for all key press sequences.

Custom Key Maps

Custom Key Maps should not be confused with the process the system administrator uses to re-map the Scan buttons on either side of the touchscreen display.

See Appendix A “Keymaps”, section titled “Creating Custom Keymaps”.

To activate the Custom keymap, select **Start | Settings | Control Panel | Keyboard** icon. Select the Custom keymap from the keyboard popup menu, and close the control panel with the OK button. To return to the default keymap, select **0409** from the keymap popup and tap OK.

Note: Mobile device’s host connection and Custom Key Maps: before connecting to a host using Remote Desktop Connection, go to ***Start | Settings | Control Panel | Keyboard*** *and select* ***0409*** *from the keymap popup. Tap OK.*

LED Functions

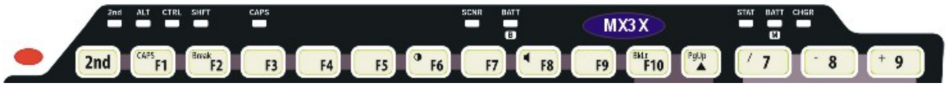


Figure 2-9 LED Functions

Across the top of the keypad are LEDs that provide visual cues to current computer operation. When the LED is not illuminated, the function is inactive.

LED	When illuminated ...
2nd	The next keypress is a 2nd keypress. • Amber when on • Blinks amber during configuration key sequence.
ALT	The next keypress is an ALT keypress. • Amber when on and unlit when off.
CTRL	The next keypress is a CTRL keypress. • Amber when on and unlit when off.
SHFT	The next letter is the uppercase letter on alpha keys and the shifted character on the numeric keypad keys. • Amber when on and unlit when off.
CAPS	Uppercase letters are active until the CAPS key sequence is pressed again. • Amber when on and unlit when off.
SCNR	Barcode scanner function, affected by both tethered scanners and the scanner endcap. • Red – scanning. • Green – good scan. • Unlit – scanner is inactive.
BATT B	Backup Battery. When illuminated, the backup battery is charging. When unlit, the backup battery is not charging
STAT	Status Indicator. • Amber – device is booting up. • Blinking Green when display Suspend state begins.
BATT M	Main Battery. When illuminated, main battery capacity is low. • Red – low battery. • Blinking Red – power fail. • Unlit – Main battery is not low OR all charge is depleted in both batteries..
CHGR	Charger. When on, the mobile device is receiving external power from the DC power jack on the endcap. • Red – Main battery is charging. • Amber – Fault or temporary standby (Contact LXE Customer Support). • Green – battery charge is complete and the mobile device is connected to external power through the power jack.

Display

The touchscreen display is an LCD unit capable of supporting VGA graphics modes. Display size is 640 x 240 pixels. The display covering is designed to resist stains. The touchscreen allows signature capture and touch input. A pen stylus is included. The touchscreen responds to an actuation force (touch) of 4 oz. of pressure (or greater).

The transmissive color display is optimized for indoor lighting. It cannot be used without the backlight. The color display has a CCFL (Cold-Cathode Fluorescent Lighting) backlight. The transmissive display appears black when the display is off.

The choice between font sizes is made in the Control Panel option **Display | Appearance**. Font size selection may be overridden by a user supplied application.

The display is automatically turned off when the System Idle timer or Suspend timer expires.

Display and Display Backlight Timer

When the System Idle timer expires the display is turned off. The default value for the battery power timer is 15 seconds. The default value for the external power timer is 2 minutes.

When the User Idle timer expires the screen display backlight is turned off. The default value for the battery power timer is 3 seconds. The default value for the external power timer is 2 minutes.

Both values can be adjusted using the Control Panel option “Display | Backlight” or “Power | Schemes”. Any of the following will wake the display and display backlight:

Any key on the keypad
Stylus touch on the touchscreen
Power button tap

When the display wakes up, the timers will begin the countdown again. When any of the above events occurs prior to the timers expiring, the timers start the countdown again.

Touchscreen

The touchscreen provides a means of inputting information into the device by touching the screen using the LXE approved stylus (the Passive Pen – see Chapter 1 section titled “Accessories.”)

Touchscreen operation is not affected by Display Backlighting.

Touchscreen operation is affected by the Display mode. If the display is off, a stylus touch on the display will turn on the display. No touch data is sent to the running application until the next stylus touch.

Cleaning the Glass Display/Scanner Aperture

Note: These instructions are for components made of glass. If there is a removable protective film sheet on the display screen, remove the film sheet before cleaning the screen.

Keep fingers and abrasive or sharp objects away from the scan aperture and display. If the glass becomes soiled or smudged, clean only with a standard household cleaner such as Windex(R) without vinegar or use Isopropyl Alcohol. Do not use paper towels or harsh-chemical-based cleaning fluids since they may result in damage to the glass surface. Use a clean, damp, lint-free cloth. Do not scrub optical surfaces. If possible, clean only those areas which are soiled. Lint/particulates can be removed with clean, filtered canned air.

Applying the Protective Film to the Display

First, clean the display of fingerprints, lint particles, dust and smudges.

Remove the protective film from it's container. Remove any protective backing from the film sheet by lifting the backing from a corner of the film. Discard the backing.

Apply the film to the screen starting at one side and smoothing it across the display. If air bubbles appear, raise the film slightly and continue smoothing the film across the display until it covers the glass surface of the display.

If dust, lint or smudges are trapped between the protective film and the glass display, remove the protective film, clean the display and apply the protective film again.

Speaker

The speaker is located on the front of the mobile device above the Power button.

The Speaker has a loudness of at least 90 dB (2700 Hz) at 10 cm measured from the front of the unit. The Speaker volume is adjustable via the keypad or the Control Panel or by an application through the use of an API call. There are 16 distinct volume levels. The minimum volume level is 0 (no sound) with a default setting of maximum non-distorted volume. The volume sticks at maximum and minimum levels.

The speaker is disabled when a headset is plugged into the Audio Jack on the endcap.

Speaker volume is enabled and adjusted using the Control Panel "Volume & Sounds" option. After the speaker has been enabled using the Control Panel option, speaker volume is adjusted using the 2nd + <F8> key sequence, if desired.

Operational "beeps" are emitted from the speaker.

Infrared (IR) Port

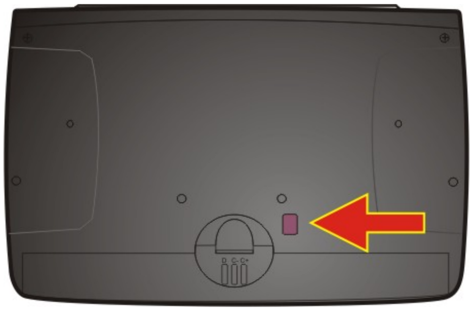


Figure 2-10 Infrared Port – COM2 Port

At the back of the mobile device is an Infrared (IR) Data Port. The IR Port is designed to provide a data link between the mobile device and a similarly equipped piece of equipment such as a printer. The IR port is the mobile device's COM 2 port and is a bi-directional half-duplex communication port. It supports baud rates up to 115k, SIR (Slow IR). It will support serial port emulation, as well as IrDA and Winsock over IR protocols. It also supports ActiveSync.

The IR operating envelope has a distance range of 2 cm (.79 inches) to 1 meter (3.2 feet) with a viewing angle of 30 degrees.

The mobile device uses IrDA protocol to send data in both directions, but not simultaneously. When sending data through the IR port, make sure the IR port on the first mobile device and the IR port on the second mobile device are in close proximity to each other. IrDA is not required and not used by terminal emulation programs.

Power Supply

Introduction

Note: *LXE recommends that the correct MX3 Multicharger Plus always be used to charge the mobile device's main battery. The Multicharger plus label is located on the back of the device and the charger must have been upgraded to V1.01 to charge the mobile device's main battery pack to 100%. Please contact your LXE representative for further information about theV1.01 upgrade kit, if needed.*

The mobile device is designed to work with a Lithium-Ion (Li-Ion) battery pack from LXE.

The mobile device receives continuous power from two batteries. There is a Lithium-Ion main battery that can be recharged separately by an LXE approved battery charging unit. The main battery is recharged, if required, while installed in a powered cradle or when the mobile device is connected to external power using the power jack. There is a 50 mAh Nickel-Cadmium (NiCd) backup battery inside the mobile device that is recharged only by the main battery.

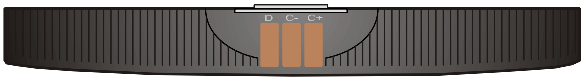


Figure 2-11 Main Battery

Note: ***New batteries must be charged prior to use**. This process takes up to four hours in an LXE Multi-Charger and eight hours when the mobile device is connected to external power through it's power jack.*

Check Battery Status

Tap the **Start | Settings | Control Panel | Power** icon. Main and backup battery level, status and Power Scheme timeout setting options are displayed.

Handling Batteries Safely

- Never dispose of a battery in a fire. This may cause an explosion.
- Do not replace individual cells in a battery pack.
- Do not attempt to pry open the battery pack shell.
- Be careful when handling any battery. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it using proper procedures.

Caution ⚠ Nickel-based cells contain a chemical solution which burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.

Caution ⚠ NiCd and Li-Ion batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a battery in a pocket or case with keys, coins, or other metal objects.

Li-Ion Battery

When disposing of the main battery, the following precautions should be observed:

The battery should be disposed of promptly. The battery should not be disassembled or crushed. The battery should not be heated above 212°F (100°C) or incinerated.

Main Battery

The main battery has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the LXE Multi-Charger Plus or the mobile device battery well.

When the main battery is properly installed in the unit it provides up to eight hours of operation depending upon operation and accessories installed. The battery pack is resistant to impact damage and falls of up to four feet to a concrete surface.

Under normal conditions it should last approximately eight hours before requiring a recharge. The more you use the scanner, the radio, or the backlight at it's brightest setting, the shorter the time required between battery recharges.

Battery Hot-Swapping

When the main battery power level is low, the mobile device will signal the user with a warning dialog box on the display and the BATT M LED illuminates red. The Batt-M LED is illuminated until the main battery is replaced, the battery completely depletes, external power is applied to the mobile device using the power jack.

You can replace the main battery by simply removing the discharged battery and installing a fully charged battery within a five minute time limit (or before the backup battery depletes).

When the main battery is removed, the mobile device automatically transitions to the Critical Suspend state. During Critical Suspend, the mobile device's backup battery will continue to power the unit for at least five minutes. Though data is retained, the mobile device cannot be used until a fully charged main battery is installed. After installing the fully charged battery, the mobile device automatically transitions to the Suspend state. To resume from the Suspend state, tap the Power button. Full operational recovery from Suspend can take several seconds while the radio is reestablishing an RF link.

If the backup battery depletes before a fully charged main battery can be inserted, the mobile device will turn OFF and the Power key must be used after the main battery is installed.

All configuration data is saved to flash memory before the mobile device powers off.

Low Battery Warning

It is recommended that the main battery be removed and replaced when it's energy depletes. When the Low Battery Warning appears perform an orderly shut down of the mobile device, minimizing the operation of any optional equipment and insuring any information is saved that should be saved.

When the mobile device is in an ON state, a low battery warning dialog box appears on the display and the Batt-M LED illuminates red.

An uninterrupted external power source (wall AC adapters or DC/DC converters) transfers power to the mobile device internal charging circuitry which, in turn, recharges the main battery and backup battery.

Note: Once you receive the Low Battery Warning, you have approximately 5 minutes to perform an orderly shutdown and replace the main battery before the unit powers off.

The Low Battery Warning will transition to Critical Suspend before the computer powers off.

Critical Suspend State

The Critical Suspend state or mode is entered because of a main battery Power failure. A main battery Power failure can occur because the battery energy has been depleted or the battery has been removed.

When the mobile device is in the Critical Suspend state the main battery LED illuminates, the System LED blinks red, all peripherals are shut down, the CPU clock is stopped, and power is removed from the PCMCIA card(s). The operating system is saving the state prior to the backup battery failing and cannot be used.

If a new fully charged main battery is installed before the backup battery fully depletes, the operating system will transition to the Suspend state. To resume operation tap the Power key.

Backup Battery

The mobile device has a backup battery that is designed to provide limited-duration electrical power in the event of main battery failure. The backup battery is a 50 mAh Nickel Cadmium (NiCd) battery that is factory installed in the unit. The need for recharging of the backup battery is automatically detected and controlled by the operating system. The energy needed to charge the backup battery is drawn from the main battery.

It takes several hours of operation before the backup battery is capable of supporting the operation of the computer. The duration of backup battery life is dependent upon operation of the mobile device, it's features and any operating applications.

The backup battery is replaced by LXE.

Note: *An uninterrupted external power source (wall AC adapters or DC/DC converters) transfers power to the mobile device's internal charging circuitry which, in turn, recharges the main battery and backup battery.*

Maintenance

Note: *Make sure there is a fully charged main battery in the mobile device* ***before*** *running the backup battery Discharge Utility. The backup battery can be discharged and charged while the mobile device is receiving external power through the power jack on the endcap.*

The NiCd backup battery should be discharged completely once or twice a year. The main battery will fully charge the backup battery. This process will allow longer life for the backup battery.

The backup battery is discharged by selecting **Start | Settings | Control Panel | Battery** and tapping the "Discharge" button. The discharge utility shows the progress of the discharging. At this time, the program can be exited while continuing the discharge process. Normal use of the mobile device can resume during the discharge, with the exception of Hot-Swapping the main battery. When the backup battery is fully discharged, the mobile device will automatically stop the discharge process and begin to recharge the backup battery.

DO NOT REMOVE THE MAIN BATTERY from the mobile device until the backup battery is completely discharged. Discharge requires approximately 1 hour and recharge requires approximately 2.5 hours.

MX3 Multi-Charger Plus Battery Charger

Note: *LXE recommends that the correct MX3 Multicharger Plus always be used to charge the main battery. The Multicharger plus label is located on the back of the device and the charger must have been upgraded to V1.01. Please contact your LXE representative for further information about the V1.01 upgrade kit, if needed.*

The LXE Multi-Charger Plus (9000A377CHGR5US) is designed to perform two functions:

- Simultaneously charge five LXE Rechargeable Lithium Ion Battery Packs in less than four hours.
- Simultaneously charge four LXE Rechargeable Lithium Ion Battery Packs in less than four hours and analyze a fifth Battery Pack (ending with the battery pack fully charged) in less than ten hours.

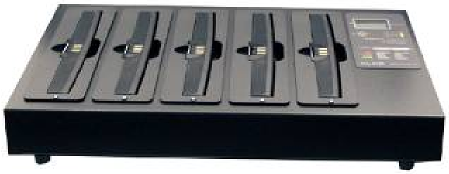


Figure 2-12 MX3 Multi-Charger Plus

The main battery can be charged in the MX3 Multi-Charger Plus. The main battery charges the backup battery using the mobile device's internal charging circuitry. The multi-charger requires an external power source.

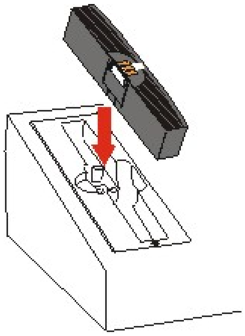


Figure 2-13 Insert Main Battery in Charge Pocket

Lower the battery pack straight into the battery charger pocket and push it down firmly until the retaining clip catches on the retaining pins. The LED at the base of the charger pocket illuminates. Refer to the *MX3 Multi-Charger Plus User's Guide* for LED explanation and troubleshooting.

Do not "slam" the battery into the charging cup or slide it in sideways. Failure to follow these instructions can result in damage to the main battery or the charger.

Chapter 3 System Configuration

Introduction

There are several different aspects to the setup and configuration of the mobile device. Many of the setup and configuration settings are dependent upon the optional features such as installed hardware and software. The examples found in this chapter are to be used *as examples only*, the configuration of your specific mobile device computer may vary. The following sections provide a general reference for the configuration of the mobile device and some of it's optional features.

Windows CE .NET 4.2

For general use instruction, please refer to commercially available Windows CE .NET user's guides or the Windows CE .NET on-line Help application installed in the mobile device.

This chapter's contents assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows 2000, NT, or XP desktop computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the mobile device and the Windows CE .NET environment.

2.4 GHz Radio Configuration

Complete 2.4GHz radio configuration is included in Chapter 4, "Wireless Network Configuration".

Installed Software

Note: Some standard Windows options require an external modem connection. Modems are not available from LXE nor supported by LXE.

When you order a mobile device you receive the software files required by the separate programs needed for operation and radio communication. The files are loaded by LXE and stored in subdirectories in the mobile device. This section lists the contents of the subdirectories and the general function of the files. Files installed in the mobile device are specific to the intended function of the mobile device.

Files installed in each mobile device configured for an RF environment contain PCMCIA card radio specific drivers – the drivers for each type of radio are specific to the manufacturer for the radios installed in the RF environment and are not interchangeable.

Software Load

The software loaded on the mobile computer consists of Windows CE .NET 4.2 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

Operating System

- Microsoft CE .NET version 4.2.

Radio Drivers

- Only one radio is installed at any one time. The 2.4GHz type of PC radio card resident in the device determines the type of radio driver running on the device.

RFID Driver

- Includes a configuration utility to be used when programming an RFID Tag reader.

Note: Please contact your LXE representative for MX3-RFID software updates as they are released by LXE.

Software Applications

The following applications are included:

- WordPad (was PocketWord in previous versions of Windows CE)
- Pocket Inbox
- Word Viewer
- Excel Viewer
- PDF Viewer
- Image Viewer
- Scanner Wedge (LXE developed)
- Transcriber
- Media Player
- Internet Explorer

Note that the viewer applications allow viewing documents, but not editing them.

JAVA (Option)

Installed by LXE. Files can be accessed by tapping **Start | Programs | JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of JAVA examples and Plug-ins is also installed with the JAVA option. LXE does not support all JAVA applications running on the mobile device.

LXE RFTerm (Option)

Installed by LXE. The application can be accessed by tapping **Start | Programs | RFTerm**. Please refer to "Terminal Emulation Setup" earlier in this guide for RFTerm quick start instruction. Refer to the "RFTerm Reference Guide" on the LXE Manuals CD for complete information and instruction.

WaveLink Avalanche (Option)

Installed by LXE. Enabler files are installed upon initial bootup and after a hard reset. The designation of the mobile device to the Avalanche CE Manager is LXE_MX3. *Not available in this release.*

Desktop

For general use instruction, please refer to commercially available CE .NET user's guides or the CE .NET on-line Help application installed in the mobile device.

The Desktop appearance is similar to that of a desktop PC running Windows 2000, NT, or XP.

At a minimum, it has the following icons that can be tapped with the stylus to access My Computer, Internet Explorer, and the Recycle Bin.

At the bottom of the screen is the Start button. Tapping the Start Button causes the Start Menu to pop up. It contains the standard Windows menu options: Programs, Favorites, Documents, Settings, Help, and Run.

The Start Menu Shutdown option found on most desktop PC's has been replaced with a single command: "Suspend" because the mobile device is always powered On (when a fully charged main battery and backup battery are present).

Tap the Suspend button to turn the screen off or tap the red Power button to turn the screen off and place the device into Suspend mode.

Tap the screen once more or tap the Power button to "wake" the unit up.

Desktop Icon	**Function**
My Computer	Access files and programs.
Recycle Bin	Storage for files that are to be deleted.
Internet Explorer	Connect to the Internet/intranet (requires radio card and Internet Service Provider – ISP enrollment is not available from LXE).
My Documents	Storage for downloaded files / applications.
Client Configuration Utility	Set up client communication with the internet and intranet.
Start	Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help, run programs or place the unit into Suspend mode.

My Computer Folders

Folder	Description	Preserved upon Reboot?
System	Internal ATA Card	Yes
Network	Mounted network drive	No
Storage Card	ATA Card in Compact Flash Slot 1	Yes
Windows	Operating System in ROM	Yes
Program Files	Applications	No
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Temp	Location for temporary files	No

Folders Copied at Startup

The following folders are copied on startup:

System\Desktop	copied to	Windows\Desktop
System\Favorites	copied to	Windows\Favorites
System\Fonts	copied to	Windows\Fonts
System\Help	copied to	Windows\Help
System\Programs	copied to	Windows\Programs

This function copies only the directory contents, no sub-folders.

The following folders are *NOT* copied on startup:

Windows\AppMgr
Windows\Recent
Windows\Startup

because copying these has no effect on the system, or an incorrect effect.

Files in the Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by Launch.

Start Menu Program Options

The following options represent the factory default program installation. Your Program options may be different based on the software and hardware options purchased. Note that there can be only one radio installed at a time. The radio driver configuration utility chosen is based on the type of installed radio card.

Access: Start | Programs

Cisco	Set Cisco client / network parameters (See Chapter 4, “Wireless Network Configuration” for instruction.)
Communication	**Stores Network communication options**
ActiveSync	Transfer files between a mobile device and a desktop computer
Connect	Run this command after setting up a connection
Start/Stop FTP Server	Start or Stop the FTP Server
Diagnostics (optional)	**Diagnostic tests for the Mobile Device**
Registry Editor	Edit the mobile device registry (carefully)
Test Utility	Select a test to run e.g. Display, keyboard, audio.
Microsoft File Viewers	**View downloaded files** (see Note)
Excel Viewer	View Excel 97 / 2000 / 2002 documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word 97 / 2000 / 2002 and RTF files
Summit	Tap the Network icon in the toolbar to set up the Summit client (See Chapter 4, “Wireless Network Configuration” for instruction.)
Command Prompt	The command line interface in a separate window
Inbox	Microsoft Outlook mail inbox.
Internet Explorer	Access web pages on the world wide internet
Media Player	Music management program
Microsoft WordPad	Opens an ASCII notepad
Remote Desktop Connection	Log on to a Windows Terminal Server.
LXE RFID Config	Configure the RFID reader.
Transcriber	Enter data using the stylus on the touchscreen.
Windows Explorer	File management program

Note: The Microsoft File Viewers cannot display files that have been password protected or encrypted.

Communication

Access: Start | Programs | Communication

Note: Some communication menu options require an external modem connection to the mobile device. Modems are not available from LXE nor supported by LXE.

ActiveSync

After a connect setup is selected, **Start | Programs | Communication | Connect** will start to connect to a host. After this connection is made and an ActiveSync relationship established, the ActiveSync menu item can be used to establish the connection over the radio link.

See Chapter 1 “Introduction” section titled “ActiveSync”.

Connect

After a connect setup is selected, **Start | Programs | Communication | Connect** will start to connect to a host. Connect is used to initiate a cabled connection to a host. Several pre-defined connect setups are included in the factory setup:

- COM1 direct connect at 57600 or 115200 baud
- Infrared connect at 57600 or 115200 baud
- COM3 direct connect at 57600 or 115200 baud
- USB direct connect

The default connect setup is USB direct connect.

Select "Make New Connection" and follow the instructions on the screen to create a connection while following the directions in the section titled "Backup Data Files using ActiveSync" later in this chapter.

See Also: Chapter 1 “Introduction”, section titled “ActiveSync”, subsection titled “Cold Boot and Loss of Host Re-connection”

Start FTP Server / Stop FTP Server

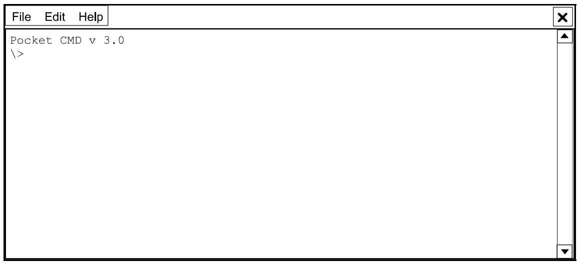
These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

Start | Programs | Communication | Start FTP Server

Start | Programs | Communication | Stop FTP Server

Command Prompt

Access: Start | Programs | Command Prompt



```
Pocket CMD v 3.0
\>
```

Figure 3-1 Pocket CMD Prompt Screen

Type help at the command prompt for a list of available commands.

Exit the Command Prompt by typing exit at the command prompt or select File | Close.

Inbox

Access: Start | Programs | Inbox

This option requires a connection to a mail server. There are a few changes in the CE .NET version of Inbox as it relates to the general desktop Windows PC Microsoft Outlook Inbox options. Tap the "?" button to access Inbox Help. ActiveSync can be used to transfer messages between the mobile device inbox and a desktop inbox.

Internet Explorer

Access: Start | Programs | Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the CE .NET version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the "?" button to access Internet Explorer Help.

Media Player

Access: Start | Programs | Media Player

There are few changes in the CE .NET version of Media Player as it relates to the general desktop Windows PC Microsoft Media Player options. Tap the "?" button to access Media Player Help.

Remote Desktop Connection

Access: Start | Programs | Remote Desktop Connection

There are few changes in the CE .NET version of Remote Desktop Connection as it relates to the general desktop Windows PC Microsoft Remote Desktop Connection options.

Select a computer from the drop down list and tap the Connect button.

Tap the **Options** >> button to access the General, Display, Local Resources, Programs and Experience tabs. Tap the "?" button to access Remote Desktop Connection Help.

Note: Custom Key Maps: before connecting to a host using Remote Desktop Connection, go to ***Start | Settings | Control Panel | Keyboard*** *and select* ***0409*** *from the keymap popup. Tap OK.*

LXE RFID Config

Note: LXE RFIDConfig is included here for backward compatibility with earlier versions of the MX3-RFID.

Access: Start | Programs | LXE RFIDConfig ***or***
Start | Settings | Control Panel | RFID

Control Panel parameters established in Power Properties affect the mobile device operating system. Power Management settings in the RFID Configuration utility governs power management of the RFID reader only.

Transcriber

Access: Start | Programs | Transcriber

Select Transcriber on the **Start | Programs** menu. To make changes to the Transcriber application, enable or disable the current Transcriber session, etc., tap the “hand with a pen” icon in the toolbar. Tap the “?” button or the Help button to access Transcriber Help.

Windows Explorer

Access: Start | Programs | Windows Explorer

There are a few changes in the CE .NET version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Tap the “?” button to access Windows Explorer Help.

Taskbar

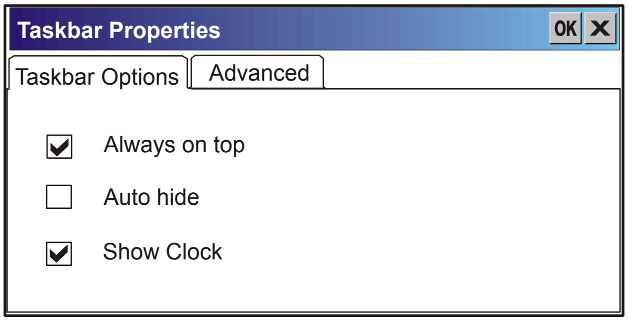
Access: Start | Settings | Taskbar and Start Menu

The Taskbar can also be accessed by tapping on the taskbar and holding the stylus on the taskbar. Choose Properties from the popup menu.

Factory Default Settings	
Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled

There are a few changes in the CE .NET version of Taskbar as it relates to the general desktop PC Windows Taskbar options.

When the taskbar is auto hidden, press the **Ctrl** key then the **Esc** key to make the Start button appear.



☑ Always on top

□ Auto hide

☑ Show Clock

Figure 3-2 Taskbar Properties

Advanced Tab

Expand Control Panel

Tap the checkbox to have the Control Panel folders appear in drop down menu format from the Settings | Control Panel menu option.

Clear Contents of Document Folder

Tap the Clear button to remove the contents of the Document folder.

Control Panel Options

Access: **Start | Settings | Control Panel** or **My Computer | Control Panel**

Getting Help

Please tap the “?” box to get Help when changing Control Panel options.

Option	Function
About	Displays hardware and software details.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Aironet Client Utility	Set the parameters for a Cisco client. (See Chapter 4, “Wireless Network Configuration” for instruction.)
Battery	View the status of the Main and Backup batteries.
Bluetooth Device	Set the parameters for a Bluetooth device. *Not available in this release.*
Certificates	Manage digital certificates used for secure communication.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings. Use Sync button to synchronize mobile device time with an internet time server.
Dialing	Set dialup properties for internal modems (modems are not supplied/supported by LXE).
Display	Set background graphic, color scheme appearance, and power scheme properties.
Input Panel	Select the current key / data input method.
Internet Options	Set General, Connection, Security and Advanced options for Internet connectivity.
Keyboard	Set key repeat delay and key repeat rate.
Mixer	Adjust the volume, record gain, and sidetone for microphone input.
Mouse	Set the double-tap sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.
Owner	Set owner details.
Password	Set access password properties.
PC Connection	Control the connection between the mobile device and a local desktop or laptop computer.
PCMCIA	Radio card in Slot 0, Internal ATA in Slot 2.
Power	Set Power Off, Backlight properties. Review battery status and perform backup battery charging/discharging.
Regional Settings	Set appearance of numbers, currency, time and date based on regional and language settings.
Remove Programs	Remove user installed programs in their entirety.

Option	Function
RFID	RFID Configuration Utility. Set Tag, Filter, Power, Read, and Format parameters. Use this option to upgrade RFID firmware.
Scanner	Set scanner keyboard wedge, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports. Use Advanced Barcode Processing.
Storage Manager	Manage storage devices, create partitions.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings.
Volume and Sounds	Set volume parameters and assign sound wav files to CE .NET events.

About

Access: Start | Settings | Control Panel | About

Displays hardware and software details.

Tab Title	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language. Language indicates any pre-installed Asian fonts.
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	LXE Utilities, LXE Drivers, LXE Image, LXE API, .NET Framework version, RFID Driver version and Internet Explorer.
Network IP	Current network connection IP and MAC address.

User application version information can be shown in the Version window. Version window information is taken from the registry.

Modify the Registry using the Registry Editor (see section titled “Utilities”). LXE recommends **caution** when editing the Registry and also recommends making a backup copy of the registry before changes are made.

The registry settings for the Version window are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

Create a new string value under this key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window.

Language and Fonts

The **Software** tab displays any fonts built into the OS image.

The fonts built into the OS image are noted in the Language section of this tab:

- English only – No additional fonts are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The above listed Asian fonts are ordered separately and built-in to the OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the (English only) default (extended) fonts.

When an Asian font is copied into the fonts folder on the /System folder; the font works for Asian web pages, the font works with RFTerm, the font does not work for Asian options in **Regional Settings** control panel, the font does not work for naming desktop icons with Asian names, the font does not work for third-party .NET applications, the font does not work for some third-party MFC applications.

Identifying Software Versions

The “Versions**”** tab displays the versions of many of the software programs installed. Not all installed software installed on the mobile device is included in this list and the list varies depending on the applications loaded on the mobile device. The LXE Image line displays the revision of the system software installed. Please refer to the last three digits to determine the revision level.

Radio MAC Address

The “Network IP” tab displays the MAC address of the radio card.

Accessibility

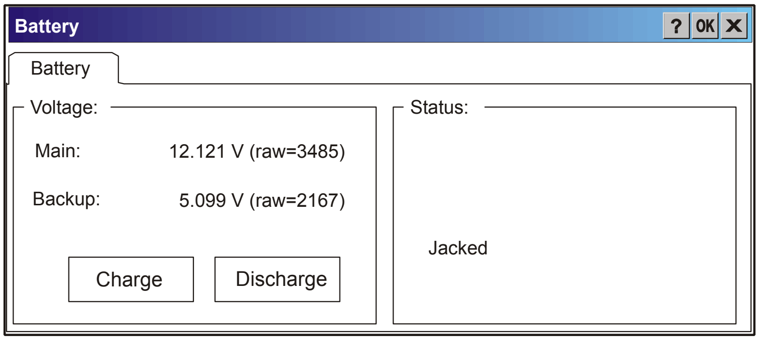
Access: Start | Settings | Control Panel | Accessibility

Customize the way the keyboard, sound, display, mouse, automatic reset and notification sound function. There is no change from general desktop Accessibility options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Battery

Access: Start | Settings | Control Panel | Battery

View the status of the Main and Backup batteries.



Voltage:

Main: 12.121 V (raw=3485)

Backup: 5.099 V (raw=2167)

Status:

Jacked

Figure 3-3 Battery

The Battery tab shows the status and the percentage of power left in the main battery (external). It also shows the status of the backup battery. The listed values cannot be changed by the user.

Tap the Charge or Discharge buttons to charge and discharge the backup battery. If the battery is Charging, tap the Discharge button to stop the Charge process. Tap Discharge a second time to begin the Discharge process. If the battery is Discharging, tap the Charge button to stop the Discharge process. Tap Charge a second time to begin the Charge process.

Bluetooth Manager

Note: May or may not be available in every MX3-RFID version. Bluetooth Manager, Bluetooth service or options are not available for all MX3-RFID devices or in all MX3-RFID software releases.

Access: Start | Settings | Control Panel | Bluetooth Device Properties

Set the parameters for a Bluetooth device.

Factory Default Settings	
All Found Devices	Untrusted

Tap the Scan Device button to locate Bluetooth devices in your wireless area. Tap the "?" button and follow the instructions in the Help file to authenticate Bluetooth devices in your area.

Certificates

Access: Start | Settings | Control Panel | Certificates

Manage digital certificates used for secure communication.

Lists the Stored certificates trusted by the mobile device user. These values may change based on the type of wireless security resident in the client, access point or the host system. See Chapter 4 "Wireless Network Security" section titled "Certificates" for instruction.

Date/Time	It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

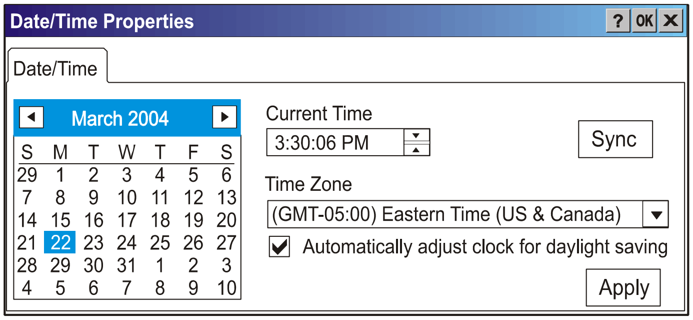
Date/Time

Access: Start | Settings | Control Panel | Date/Time Icon

Set Date, Time, Time Zone, and Daylight Savings after cold boot or at anytime.

Factory Default Settings	
Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Disabled

Note: Date and time is reset to the default value each time the mobile device is rebooted.



Date/Time Properties

Date/Time

March 2004

S	M	T	W	T	F	S
29	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

Current Time: 3:30:06 PM

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

☑ Automatically adjust clock for daylight saving

Figure 3-4 Date/Time Properties

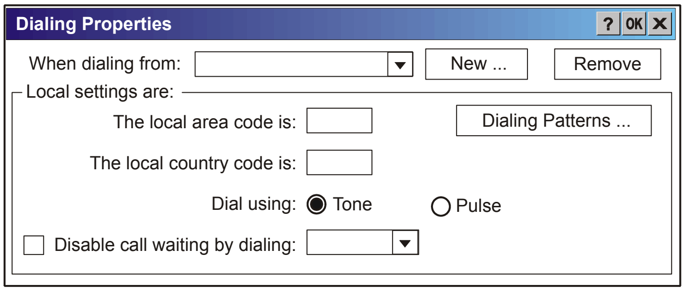
There is no change from general desktop PC Date/Time Properties options. Adjust the settings and tap the OK box or the Apply button to save the changes. The changes take effect immediately. Double-tapping the time displayed in the Taskbar causes this display to appear.

Sync requires Internet connection. When an Internet connection is available, tap the Sync button to synchronize the mobile device operating system time with an Internet time server.

The MX3-RFID includes a **GrabTime** utility which can be configured to synchronize the time at each boot up. Please see “Enabling GrabTime”, in the “Utilities” section, for details.

Dialing

Access: Start | Settings | Control Panel | Dialing



Dialing Properties

When dialing from:

Local settings are:

The local area code is:

The local country code is:

Dial using: ● Tone ○ Pulse

□ Disable call waiting by dialing:

Figure 3-5 Dialing

Set dialup properties for internal modems (modems are not supplied/supported by LXE). Tap the “?” and follow the instructions in Help.

Display

Access: Start | Settings | Control Panel | Display Icon

Set background graphic, color scheme appearance, and power scheme properties.

Note: Control Panel parameters established in Display Properties, Power Properties and Volume & Sounds Properties remain in effect during RFID configuration and the resulting read functions.

Factory Default Settings	
Background	Windows CE
Tile	Disable
Appearance	
Scheme: Monochrome Color	 High Contrast White Windows Standard
Backlight	
Battery Power Auto Turn Off	Enabled
Idle Time	3 Seconds
External Power Auto Turn Off	Enabled
Idle Time	2 minutes

Background

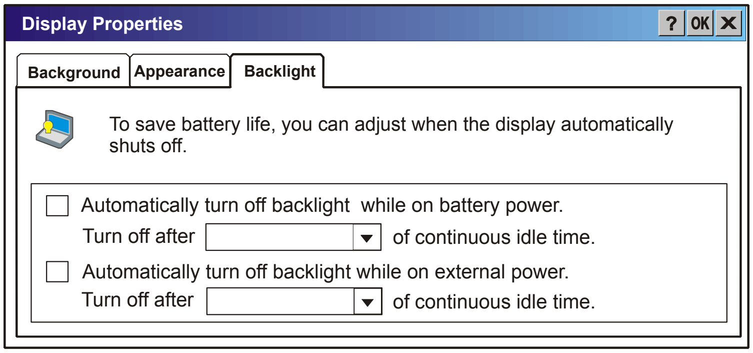
There is no change from general desktop PC Display Properties / Background options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Appearance

No change from general desktop PC Display Properties / Appearance options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately. The default is Windows Standard for color displays.

Note: The color screens display Windows standard colors (or the color scheme selected) instead of shades of grey.

Backlight



To save battery life, you can adjust when the display automatically shuts off.

□ Automatically turn off backlight while on battery power.
Turn off after [▼] of continuous idle time.
□ Automatically turn off backlight while on external power.
Turn off after [▼] of continuous idle time.

Figure 3-6 Display Properties / Backlight Tab

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately. When the backlight timer expires, the color transmissive backlight is dimmed -- not turned off.

Input Panel

Access: Start | Settings | Control Panel | Input Panel

Select the current key / data input method.

Factory Default Settings	
Input Method	Keyboard
Allow applications to change input panel state	Disabled
Keys	Small keys
Use gestures	Disabled

Use this option to make the Soft Keyboard or the integrated keypad primarily available when entering data. Selecting Keyboard enables both.

Enable the input panel by checking “Allow applications to change the input panel’s state”. Then tap the OK button. Warmboot the device to store the changed setting.

Internet Options

Access: Start | Settings | Control Panel | Internet Options

Set General, Connection, Security and Advanced options for internet connectivity.

Factory Default Settings	
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512 Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Advanced	
Display web images	Enabled
Play web sounds	Enabled
Enable web scripting	Enabled
Display script error note	Disabled
Underline links	Never

Select a tab. Adjust the settings and tap the OK box to save the changes. Tap the Clear Cache or Clear History buttons to clear files that have been downloaded to the mobile device during internet use. The changes take effect immediately. Help is not available for this option.

Keyboard

Access: Start | Settings | Control Panel | Keyboard Icon

Set key repeat delay and key repeat rate.

Factory Default Settings	
Repeat	Enable
Delay	Short
Rate	Slow
Key Map	0409

There is no change from general desktop PC Keyboard Properties options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

When new key maps are added to the registry, they appear in the Key Map dropdown list on the Keyboard Panel.

These values do not affect virtual keyboard taps.

Mixer

Access: Start | Settings | Control Panel | Mixer Icon

Adjust the volume, record gain, and sidetone for microphone input or headphone use.

Factory Default Settings	
Master Volume	0dB
Record Gain	22.5dB
Sidetone	12.0dB
Input	None

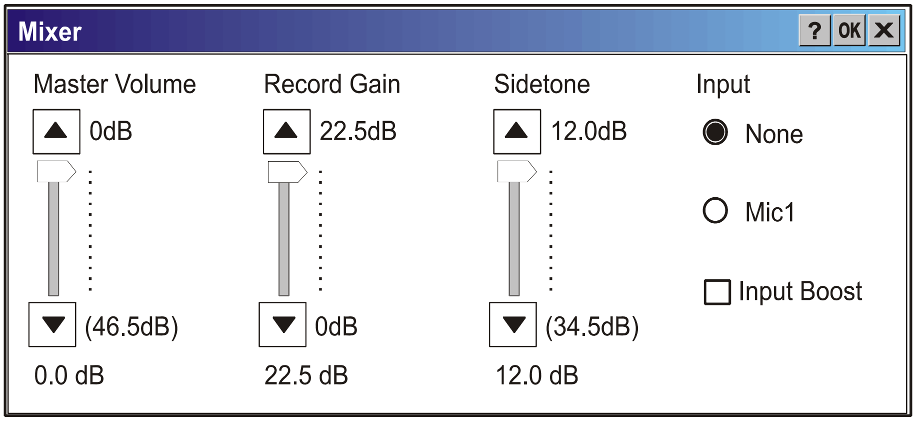


Figure 3-7 Mixer

Select the Input for the mixer. Move the sliders to adjust the decibel level. Tap OK to save the settings.

Note: Set Input to "None" when using stereo headphones. Set Input to "Mic1" when using a mono headset with microphone.

Mouse

Access: Start | Settings | Control Panel | Mouse

Set the double-tap sensitivity for stylus taps on the touchscreen.

Network and Dialup Connections

Access: Start | Settings | Control Panel | Network and Dialup Connections

Create a dialup, direct, or VPN connection on the mobile device. To configure the mobile device to use DHCP or a fixed IP address, select the desired connection. The default is to obtain an IP address via DHCP.

A static IP address can be assigned by tapping the **Specify an IP address** radio button and entering the desired IP address, subnet mask and gateway.

Create a Connection Option

1. On the mobile device, select **Start | Settings | Control Panel | Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the one you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (IR @ 9600, etc.). Tap the **Direct Connection** radio button. Tap the Next button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the **Port Settings** tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off **Wait for dial tone**, since a direct connection will not have a dial tone. Set the timeout parameter (default is 90 seconds). Tap OK.
8. **TCP/IP Settings** should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select **Start | Settings | Control Panel | PC Connection** and tap the **Change** button.
11. Select the new connection. Tap OK twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the mobile device with the appropriate cable.
14. Tap the desktop Connect icon to test the new connection.

You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

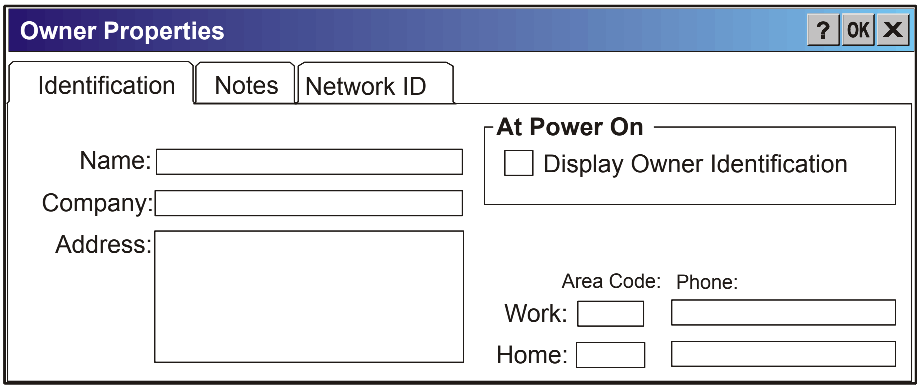
Owner

Access: Start | Settings | Control Panel | Owner Icon

Set mobile device owner details.

Factory Default Settings	
Identification	Blank
Notes	Blank

There is no change from general desktop PC Owner Properties display. Enter the information and tap the OK box to save the changes. The changes take effect immediately.



Owner Properties

Identification | Notes | Network ID

Name:

Company:

Address:

At Power On

□ Display Owner Identification

Area Code: Phone:

Work:

Home:

Figure 3-8 Owner Properties

Password

Access: Start | Settings | Control Panel | Password Icon

Set user access and power up password properties.

Factory Default Settings	
Password	Blank
At Power On	Disabled

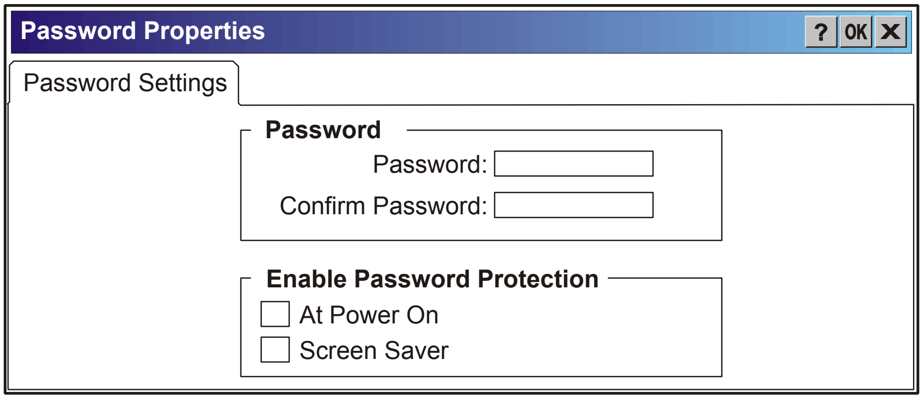
Note: Once a password is assigned, each Control Panel option requires the password be entered before the Control Panel option can be accessed. If you forget the password, it cannot be restored without performing a cold boot on the unit (which erases all memory).

Enter the password, then type it again to confirm it and tap the OK box to save the changes. The password is immediately in effect.

Tap the **Power On** checkbox to set whether the user types a password at Power On.

Tap the **Screen Saver** checkbox to set whether the user types a password to clear the screensaver. If there is no screensaver chosen, this checkbox is ignored. The screensaver password affects the Remote Desktop screensaver only.

Note: Screensavers are not installed by LXE.



Password Properties

Password Settings

Password

Password:

Confirm Password:

Enable Password Protection

□ At Power On

□ Screen Saver

Figure 3-9 Password Properties

PC Connection

Access: Start | Settings | Control Panel | PC Connection

Control the connection between the mobile device and a nearby desktop/laptop computer.

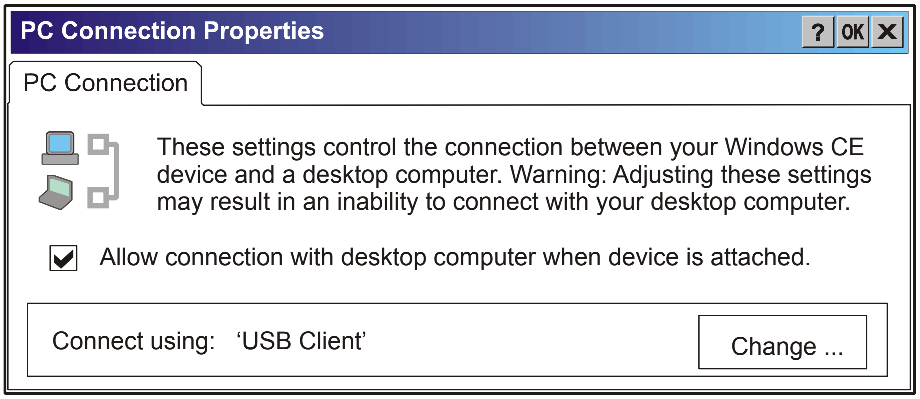
Factory Default Settings	
Allow Connection	Enabled
Connect Using	'USB Client'

Tap the Change button to adjust the settings and tap the OK button to save the changes. The changes take effect immediately.

Unchecking the "Allow connection with ….." disables ActiveSync.

Change ….

Tapping the Change button shows a list of configured ActiveSync connections. In addition, there is a checkbox for Automatic Connect. If this checkbox is checked, when the serial driver detects a cable connection on the configured port, it will automatically try to start ActiveSync on that port. Note that this interferes with processes on the configured port at the same time.



These settings control the connection between your Windows CE device and a desktop computer. Warning: Adjusting these settings may result in an inability to connect with your desktop computer.

☑ Allow connection with desktop computer when device is attached.

Connect using: 'USB Client'

Figure 3-10 Communication / PC Connection Tab

Please refer to the "Backup Data Files using ActiveSync" section later in this chapter for parameter setting recommendations.

PCMCIA

Access: **Start | Settings | Control Panel | PCMCIA**

Note: Radio card in Slot 0, Internal ATA in Slot 2.

Factory Default Settings	
Slot 0	**PCMCIA**
Disable slot now	Off
Power slot during sleep (3.3v)	Off
Power slot during sleep (5v)	Off
Write protect slot	Off
Slot 1	**Compact Flash**
Disable slot now	Off
Power slot during sleep (3.3v)	Off
Power slot during sleep (5v)	Off
Write protect slot	Off
Slot 2	**ATA Card**
Disable slot now	Off
Power slot during sleep (3.3v)	Off
Power slot during sleep (5v)	Off
Write protect slot	Off

The name of the card (from the CIS data on the card) in the slot is displayed. This information cannot be changed by the user.

When “Power slot during sleep” is checked, the slot will stay powered up in Suspend at the cost of reduced battery life.

When “Disable slot now” is checked, the slot is powered down as soon as the Control Panel is closed and the PCMCIA driver ignores any card in the slot.

Power

Access: **Start | Settings | Control Panel | Power**

Set Power Off, Backlight properties. Review battery status and perform backup battery charging/discharging.

Note: Control Panel parameters established in Power Properties affect the mobile device operating system. Power Management settings in the RFID Configuration utility governs power management of the RFID reader only.

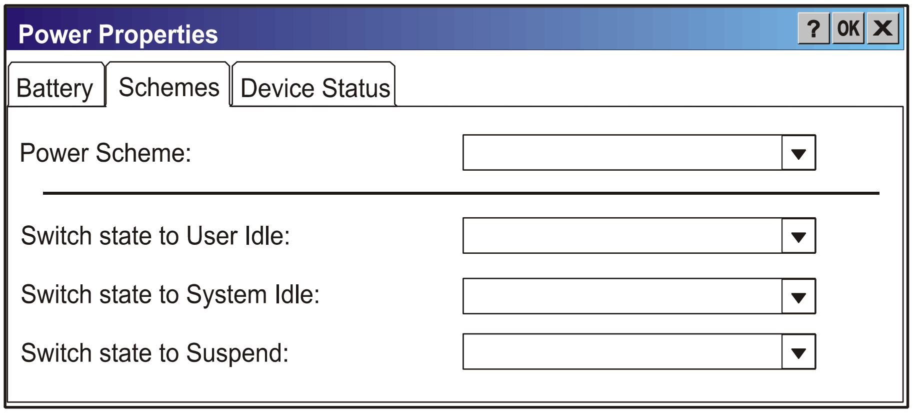
Factory Default Settings	
Battery	N/A
Schemes – Battery Power	
User Idle	3 seconds
System Idle	15 seconds
Suspend	5 minutes
Schemes – AC Power	
User Idle	2 minutes
System Idle	2 minutes
Suspend	5 minutes

Please refer to Chapter 2 "Physical Description and Layout" section titled "Power Modes".

Battery

The Battery tab shows the status and the percentage of power left in the main battery (removable). It also shows the status of the internal backup battery. The listed values cannot be changed by the user.

Schemes



Power Scheme:

Switch state to User Idle:

Switch state to System Idle:

Switch state to Suspend:

Figure 3-11 Power Schemes

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

These mode timers are cumulative. The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired. When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

Because of the cumulative effect, and using the Battery Power Scheme default settings:

The backlight turns off after 3 seconds of no activity,

The display turns off after 18 seconds of no activity (15sec + 3sec),

And the device enters Suspend after 5 minutes and 18 seconds of no activity.

Battery Power Scheme

Use this option when the device will be running on battery power only.

Switch state to User Idle:	Default is After 3 seconds
Switch state to System Idle:	Default is After 15 seconds
Switch state to Suspend:	Default is After 5 minutes

AC Power Scheme

Use this option when the device will be running on external power (e.g. AC adapter, auto outlet adapter, powered cradle).

Switch state to User Idle:	Default is After 2 minute
Switch state to System Idle:	Default is After 2 minutes
Switch state to Suspend:	Default is After 5 minutes

Device Status

This option displays the power levels being used by the mobile device.

Regional Settings

Access: Start | Settings | Control Panel | Regional Settings

Set the appearance of numbers, currency, time and date based on regional and language settings.

No change from general desktop PC Regional Settings Properties options. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Factory Default Settings	
Regional Setting	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long

Options (and defaults) for the regional settings depend on the fonts included in the OS image. Please refer to the section on the **About** control panel earlier in this chapter for more details.

Remove Programs

Access: Start | Settings | Control Panel | Remove Programs

No change from general desktop Remove Programs options. Select a program and tap the Remove button. Follow the prompts on the screen to uninstall ***user-installed only*** programs. The change takes effect immediately.

RFID Configuration Utility

Access: Start | Settings | Control Panel | RFID

Note: Control Panel parameters established in Display Properties, Power Properties and Volume & Sounds Properties remain in effect during RFID configuration and the resulting read functions.

There are two versions of the RFID Configuration Utility.

The version presented in this chapter supersedes the version installed in earlier versions of the MX3-RFID mobile device. Contact your LXE representative for availability of the previous or current RFID CAB file.

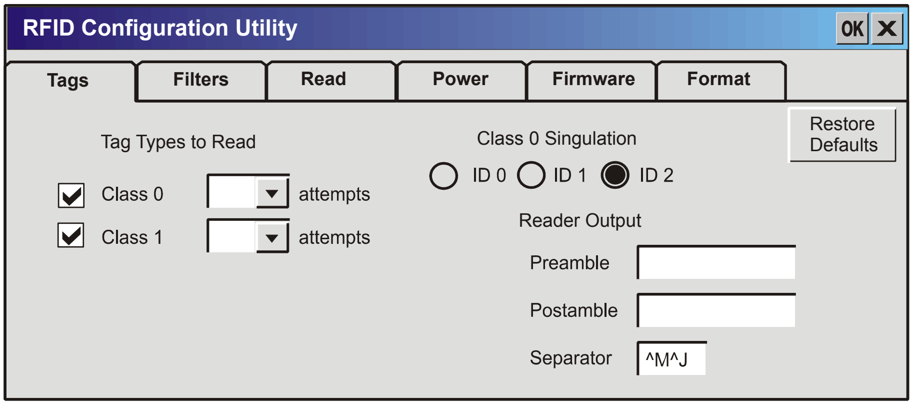
Factory Default Settings	
Tags	
Tag Types to Read – Class 0	Enabled
Class 0 Tag Read Attempts	4
Tag Types to Read – Class 1	Enabled
Class 1 Tag Read Attempts	1
Class 0 Singulation	ID 2
Tag Types to Read – C1G2	Enabled
C1G2 Tag Read Attempts	1
C1G2 Q-Value	3
Reader Output Preamble	Blank
Reader Output Postamble	Blank
Reader Output Separator	^M^J
Filters	
Select	Blank
Field Name	Blank
Offset	Blank
Mask Value	Blank
Read	
Read Once on Key Press	Enabled
Read Continuous during Key Press	Disabled
Toggle On/Off with Key Press	Disabled
Beep Once on Tag Read	Enabled
Buzz during Read Cycle	Enabled
Send Key Messages (Wedge)	Enabled
Power	
Output Power	+30 dBm
Modulation	95%
Power Management	3 sec
Disable	Disabled
Firmware	
File	Blank
Format	
HEX	Enabled
EPC	Disabled
Field Separator	Blank

See Also: “Set the Display Backlight Timer”, “Set the Power Schemes Timers”, and “Set the Audio Speaker Volume”.

Tags

Note: An MX3-RFID manufactured before August 2006 may require an update to support Class 1 Gen 2 tags. Please contact your LXE representative for assistance.

Access: Start | Settings | Control Panel | RFID | Tags tab



Tag Types to Read

☑ Class 0 attempts

☑ Class 1 attempts

Class 0 Singulation

○ ID 0 ○ ID 1 ● ID 2

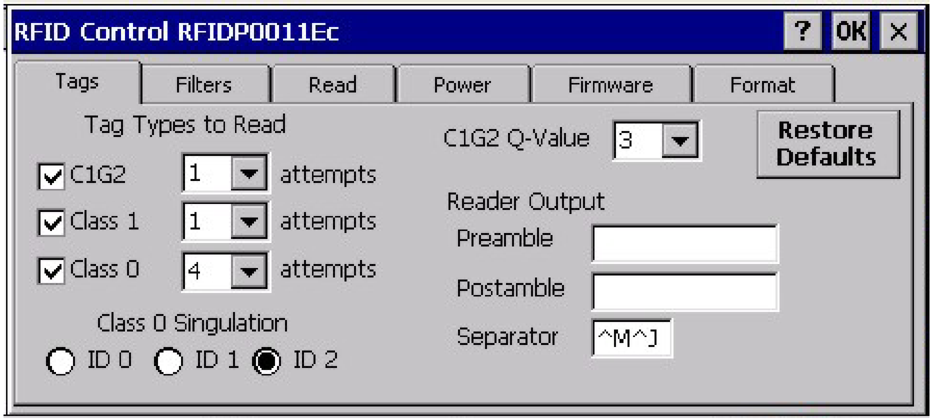
Reader Output

Preamble

Postamble

Separator ^M^J

Or



Tag Types to Read

☑ C1G2 1 attempts

☑ Class 1 1 attempts

☑ Class 0 4 attempts

Class 0 Singulation

○ ID 0 ○ ID 1 ● ID 2

C1G2 Q-Value 3

Reader Output

Preamble

Postamble

Separator ^M^J

Figure 3-12 RFID Configuration Utility – Tags tab

Note: MX3-RFID is restricted to 95% for Modulation. LXE recommends using the default setting of ID2 for Class 0 Singulation.

Data output from tags read is sent in character mode to the keyboard buffer. A pop up option box is displayed if the user attempts to deselect all tags. At least one class must be selected before the user can continue.

Tap the Restore Defaults button to set the parameters in the RFID Configuration Utility menu panels to their factory default settings.

Tag Types to Read

Specify which class of tags are to be read and reported during tag reading operations. Duplicate tags are not reported.

- Class 0 (Class 0 Read attempts)
- Class 1 (Class 1 Read attempts)
- Class 1 Gen2 (C1G2 Read attempts)

A read operation can contain a user-defined number of read attempts. The default for Class 0 tags is 4 read attempts. This means that when a read operation is performed by pressing the RFID Read button, 4 reads will be performed internally; the results merged, duplicate tags removed, and the result is then made available to the application.

Default number of reads for collecting Class 0 tags is 4. Valid values are between 1 and 10.

Default number of reads for collecting Class 1 tags is 1. Valid values are between 1 and 10.

Default number of reads for collecting Class 1 Gen 2 tags is 1. Valid values are between 1 and 10.

Change the attempts value by tapping the drop down list box and selecting a number from the list. Tap OK to save the change or X to ignore the change and return to the Control Panel. Tap the Restore Defaults button to return to default values.

C1G2 Q-Value

When scanning large numbers of tags, the C1G2 Q-value sets the amount of time to delay when sending tag reads to the keyboard buffer. A larger number increases the time delay interval. The default value is 3. Valid values are between 0 and 15.

Class 0 Singulation

Tap the radio button to specify which singulation method to use during Class 0 read operations. Selection is grayed out if the Class 0 Tag Type is unchecked. Tap OK to save the change or X to ignore the change and return to the Control Panel.

Reader Output

Preamble

A preamble is a lead-in character for tags transmitted to the host device. The lead-in characters are considered part of the tag.

The Preamble field will accept up to 5 characters that can be specified by a combination of 7-bit ACSII characters and “hat” encoded characters.

Postamble

A postamble is a follow-on character for tags transmitted to the host device. The follow-on characters are considered part of the tag.

The Postamble field will accept up to 5 characters that can be specified by a combination of 7-bit ACSII characters and “hat” encoded characters.

TAG data separators

Use data separators to add spacing between read tags. Up to 2 characters that can be specified by a combination of 7-bit ACSII characters and “hat” encoded characters.

For example, ^M^J places a carriage return (^M) and line feed (^J) after each tag is successfully read.

When the maximum number of characters is exceeded, the mobile device beeps and will not allow more characters to be entered. However, “hat” encoded characters count as a single character in determining the number of characters entered into the field. Tap OK to save the change or X to ignore the change and return to the Control Panel.

See Also: “Hat Encoding”.

Filters

Access: Start | Settings| Control Panel | RFID | Filters tab

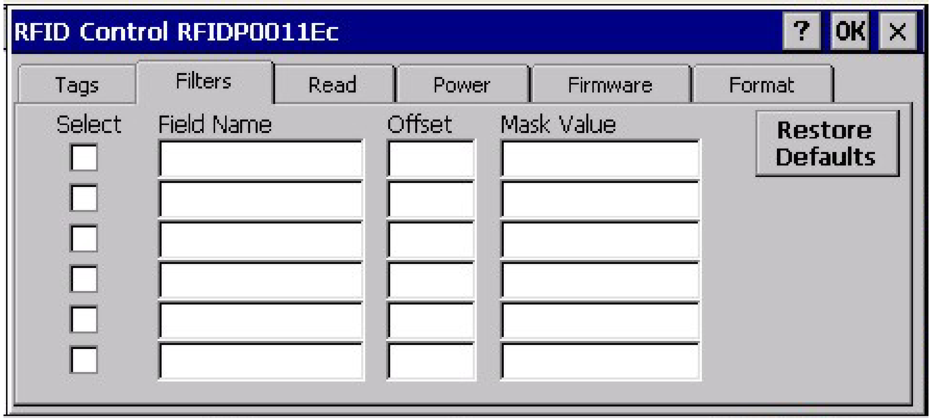


Figure 3-13 RFID Configuration Utility – Filters tab

Tap the Restore Defaults button to set the parameters in the Filters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Parameters

Default value for all parameters is blank. Tags read and reported are filtered through a logical OR of the selected mask values.

Select	Toggles between a blank and a checkmark. A checkmark in this field allows the filter on that line to be active at the next and subsequent tag read action.
Field Name	The user-friendly name for the filter. Accepts up to 40 alphanumeric characters. Field is not case sensitive. Duplicate field names are allowed between filters.
Offset	The number of characters that offset the mask value from the beginning of the tag. The range is from 0 to 23 (characters).
Mask Value	Accepts up to 24 hexadecimal characters. Field is not case sensitive. Duplicate mask values are allowed between filters. When filtering EPC decoded tags, the filter is applied before the tag is converted to EPC.

When the maximum number of characters is exceeded, the mobile device beeps and will not allow more characters to be entered.

See Also: “Decimal-Hexadecimal Chart”.

How to Set a Filter

Occasionally, it is desirable to see only a subset of tags; for example, when inventorying items from a specific company. In cases like this, filtering can be used to select only the desired tags.

1. To set up a filter, first enter a Field Name for the filter. The Field Name is simply a descriptive name that is used to distinguish the filter from other filters. In the example described previously, the Field Name could be the company name of the tags to be identified.
2. Next, enter the offset that the mask will be applied to in the Offset field. A mask value may be blank. When a blank mask value is selected as a filter it will return all tags read.
3. Then, enter the hexadecimal characters to search for in the Mask Value field.
4. Enable the filter by checking the Select field.

When the format of the tag data sent to the application is set to EPC, the filter is applied to the tag data before the conversion from hexadecimal notation to EPC format.

For example, suppose the following three tags exist:

Tag 1	c80507a000819530
Tag 2	c80507a00081a1df
Tag 3	c80507a00081a985

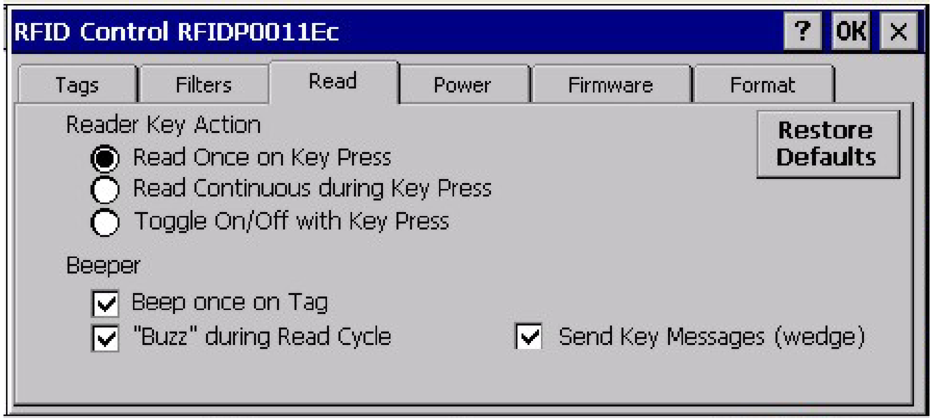
Only tags 2 and 3 are wanted from the list above.

Two filter examples to identify the “81a” tags might be:

Field Name	Offset	Mask Value
Filter 1	0	c80507a00081a
Filter 2	10	81a

Read

Access: **Start | Settings | Control Panel | RFID | Read tab**



Reader Key Action

● Read Once on Key Press

○ Read Continuous during Key Press

○ Toggle On/Off with Key Press

Beeper

☑ Beep once on Tag

☑ "Buzz" during Read Cycle

☑ Send Key Messages (wedge)

Figure 3-14 RFID Configuration Utility – Read tab

Tap the Restore Defaults button to set the parameters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Reader Key Action

When the “Toggle On/Off with key press” is enabled, the “’Buzz’ during Read Cycle” check box is automatically enabled.

Read Once on Key Press

When the RFID Read button is pressed a single read operation is performed and the RFID reader waits for another key press. The operation reads a combination of Class 0, Class 1 and C1G2 tags depending on whether the class was selected on the Tags tab. The read for each tag class consists of 1 or more internal read attempts as specified on the Tags tab.

Read Continuous During Key Press

When the RFID Read button is pressed, the MX3-RFID reads a combination of Class 0, Class 1 and C1G2 tags repeatedly until the Read button is released. The operation continuously reads a combination of Class 0, Class 1 and C1G2 tags depending on whether the class was selected on the Tags tab. The read for each tag class consists of continuous internal read attempts as specified on the Tags tab.

Toggle On/Off with Key Press

When the RFID Read button is pressed, the MX3-RFID reads a combination of Class 0, Class 1 and C1G2 tags repeatedly. It continues to perform read operations after the Read button is released and does not stop reading until the Read button is pressed again. The Read operation is cancelled. The operation continuously reads a combination of Class 0, Class 1 and C1G2 tags depending on whether the class was selected on the Tags tab.

Beeper

- Beep once on any successful read cycle (one or more Tags read)
- “Buzz” (continuous beeps) during Read Cycle.

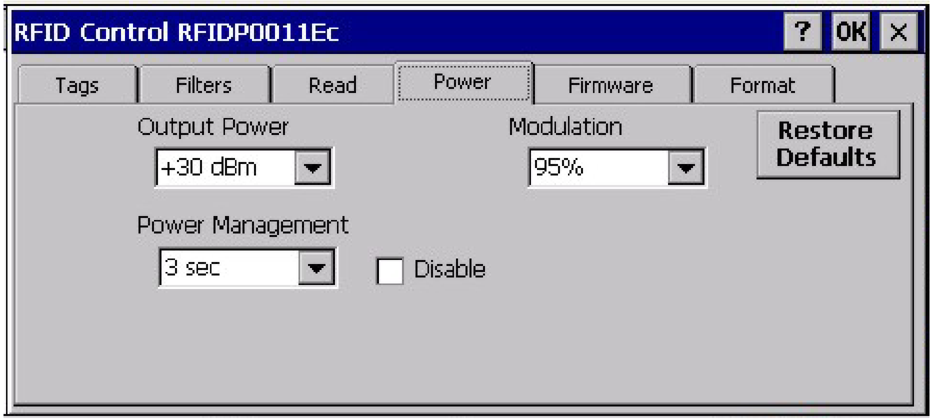
Settings	**Read Result**	
	Tag(s) Read	**No Tags Read**
Beep On / Buzz On	Beep	Buzz
Beep On / Buzz Off	Beep	No sound
Beep Off / Buzz On	Buzz	Buzz
Beep Off / Buzz Off	No sound	No sound

Power

Access: Start | Settings | Control Panel | RFID | Power tab

Note: Control Panel parameters established in Power Properties affect the mobile device operating system. Power Management set using RFID Configuration governs power management of the RFID module only.

See Also: "Set the Power Schemes Timers".



Output Power: +30 dBm

Modulation: 95%

Power Management: 3 sec

□ Disable

Figure 3-15 RFID Configuration Utility – Power tab

Tap the Restore Defaults button to set the parameters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Note: MX3-RFID is restricted to 95% for Modulation. LXE recommends using the default setting of ID2 for Class 0 Singulation.

Output Power

Provides configuration for the output power applied during Read (or Write) operations. The range is 16 settings from +15dBm to +30dBm.

Modulation

Provides configuration carrier modulation during Read (or Write) operations. The range is from 20% to 95% in 2.42% steps.

Power Management

The time out period sets the time that the software will change the RFID module state from Standby to Disable in order to reduce battery current consumption.

This timer expires if no reads have been requested for the specified period of time. The increments of the timer are 3 sec., 4 sec., 5 sec., 10 sec., 15 sec., 20 sec., 30 sec., 45 sec., 1 min., 2 min., 3 min., 4 min., 5 min., 6 min., 7 min., 8 min., 9 min., 10 min., 11 min., 12 min., 13 min., 14 min., and 15 minutes.

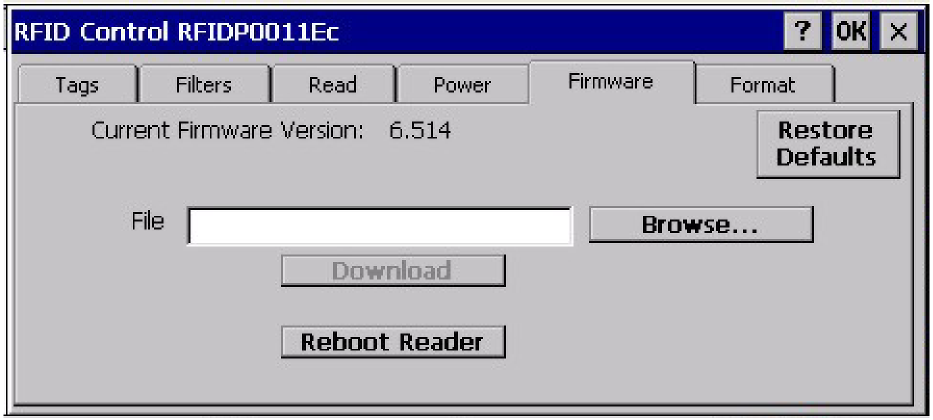
When the "Disable" check box is checked, then Power Management is disabled and the RFID module remains in the "Standby" state.

Firmware

Access: Start | Settings | Control Panel | RFID | Firmware tab

Select and install RFID firmware upgrades to the RFID module. The upgrade file is selected using standard Windows functions.

The currently loaded RFID firmware version is displayed. This value cannot be edited by the user.



RFID Control RFIDP0011Ec

Current Firmware Version: 6.514

File

Figure 3-16 RFID Configuration Utility – Firmware tab

Note: RFID firmware upgrades and subsequent rebooting does not directly cause changes to any other firmware.

Tap the Restore Defaults button to set the parameters to their last saved default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Firmware Upgrade

Tap the Browse button to locate the Firmware Upgrade File on the mobile device to download to the RFID module. Tap OK in the File Open box to select the file.

Once selected, tap the Download button on the Firmware panel. The upgrade is installed.

When the upgrade process is complete, a pop up dialog box appears indicating a successful or unsuccessful upgrade.

Tap OK in the pop up dialog box to close the dialog box.

Reboot Reader

Tap the Reboot Reader button. The RFID Reader module reboots. The MX3-RFID is not rebooted, only the RFID Reader is rebooted.

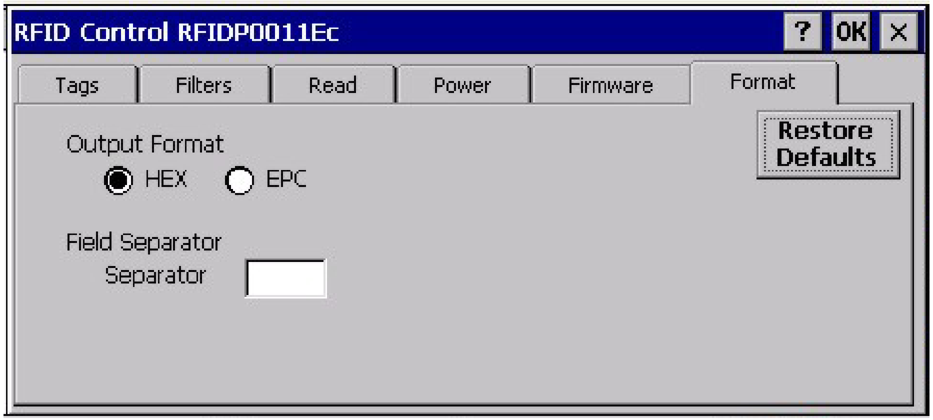
A pop up dialog box appears indicating a successful or unsuccessful reboot. The mobile device does not reboot.

Tap OK in the pop up dialog box to close the dialog box.

Format

Access: Start | Settings | Control Panel | RFID | Format tab

Use this option to select the output format that is sent to the open file from RFID read actions.



RFID Control RFIDP0011Ec

Output Format

● HEX ○ EPC

Field Separator

Separator

Figure 3-17 RFID Configuration Utility – Format tab

The default output format is HEX. When HEX is selected, the value of the Separator places the separator between each 4 characters of the outputted hexadecimal tag value.

When EPC is selected, the user can enter a field separator to use between RFID tag read actions.

There are four EPC encoding schemes available:

- SGTIN-96
- SGTIN-64
- SSCC-64
- SSCC-96

Invalid or non-supported formats are represented in HEX digits that represent the bits of encoded data read from a tag. Select EPC to decode the HEX digits into EPC tag data standards.

Tap the Restore Defaults button to set the parameters to their factory default setting. Tap OK to save changes or X to ignore any changes and return to the Control Panel.

Scanner

Access: Start | Settings | Control Panel | Scanner

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in the MX3-RFID. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain the most current software and drivers for your mobile device.

Use the Scanner panel options to set scanner keyboard wedge parameters, active scanner port, scan key settings and barcode manipulation options. Assign baud rate, parity, stop bits and data bits for available COM ports.

Factory Default Settings	
Main	
Port 1	COM1 Internal
Port 2	RFID Internal (dimmed)
Output Enable	Disabled
Power Port 1 while asleep	Disabled
Send Key Messages	Enabled
Keys	
Left	Scan
Right	RFID
COM Ports (COM1- COM2 – COM3)	
COM1	115200bps, 8 data bits, no parity, 1 stop bit (dimmed)
COM2	9600bps, 8 data bits, no parity, 1 stop bit
COM3	9600bps, 8 data bits, no parity, 1 stop bit
Power on Pin 9	Enabled
Advanced *or* **Barcode**	
Advanced Barcode Processing	Disabled

Notes:

- If the internal scanner has to be configured to operate at any communication settings other than 9600, N, 8, 1 and the MX3-RFID either loses power or a cold boot command is entered, the Scanner applet must be reconfigured to match the scanner communication settings.
- ActiveSync will not work over a COM port if that COM port is enabled in the Scanner applet as scanner input. For example, if COM 1 is being used by the scanner, COM 1 can't be used by any other program.
- The barcode scanner won't function while the RFID tag reader completes the read / accept or reject process.
- The RFID reader won't function while the barcode scanner completes the read / accept or reject process.
- Bluetooth Manager, Bluetooth service or options are not available for all devices or in all software releases.

Main Tab

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in the MX3-RFID. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain current software and drivers for your mobile device.

Parameter	Default	Options
Port 1	Internal	Disabled, COM1, COM3, Internal, Cradle, Bluetooth, Output Enable.
Port 2	RFID Internal	Disabled, RFID Internal, COM3, Internal, Cradle, Bluetooth, Output Enable
Power Port 1 while Asleep	Disabled	Enabled, Disabled. If "Power Port 1 while asleep" is checked, whichever serial port is enabled as Port 1 will remain powered while the device is in Suspend, at the cost of reduced battery life.
Send Key Messages	Enabled	Enabled, Disabled. If "Send Key Messages …" is checked any data scan is converted to keystrokes and sent to the active window. When this box is not checked, the application will need to use the set of LXE Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using "Wedge".

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Keys Tab

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in the MX3-RFID. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain current software and drivers for your mobile device.

Parameter	Default	Options
Left Scan Key	Scan	Disabled, Scan, Enter key, Tab key, Field Exit key, Virtual key, RFID (or RFID Read)
Right Scan Key	RFID	Disabled, Scan, Enter key, Tab key, Field Exit key, Virtual key, RFID (or RFID Read)

The Keys tab sets up what happens when one of the Scan keys are pressed. Note that both keys can do the same or different functions.

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Assigned	Function
Disabled	When either scan key is set to Disabled, the mobile device does nothing when pressed.
Scan	When set to “Scan” the integrated scanner is activated. If no integrated scanner is present, the Scan selection is greyed out. When using the RFID module, the Scan key defaults to the Left Scan button.
Enter	When set to “Enter”, both the Enter key and the (Scan button) / Enter key perform the same function.
Tab	When set to “Tab”, both the Tab key and the (Scan button) / Tab key perform the same function.
Field Exit	**5250 devices only**. When a Scan key is set to “Field Exit”, the key press causes the cursor to exit an input field. A field exit key press functions as a Pause key press on non-5250 devices.
Virtual	When set to “Virtual”, the Virtual Left scan key produces an F20 and the Virtual Right scan key produces an F21.
RFID	When enabled, the Right Scan / Left Scan key functions as the RFID tag reader trigger.

Change a Virtual Key (F20 or F21) Value

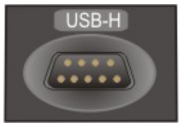
Modify the Registry using the Registry Editor (see section titled “Utilities”). LXE recommends **caution** when editing the Registry and also recommends making a backup copy of the registry before changes are made.

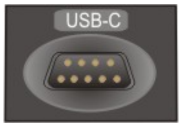
Go to HKEY_LOCAL_MACHINE \ Software \ LXE \ Scanner.

Set either the ScanCodeLeft or ScanCodeRight to be the scan code of the key to be used as the virtual key when the Virtual Left key (Left Scan key) or Virtual Right key (Right Scan key) is pressed. The registry requires a decimal value.

COM1, COM2, COM3 Tabs

Do not connect a tethered scanner to the USB labelled ports:





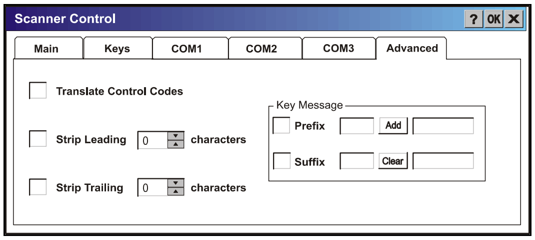
COM	Default	Options
COM1	MX3-RFID (pre-set and dimmed) – 115200, 8 data bits, 1 stop bit, no parity, Power on pin 9 enabled	Baud Rate – 115200 (RFID only), 38400, 19200, 9600, 4800, 2400, 1200 Data Bits – 8, 7 Stop Bits – 1, 2 Parity – None, Odd, Even, Mark, Space
COM2	9600, 8 data bits, 1 stop bit, no parity Power on pin 9 (+5v) Disabled	Baud Rate – 38400, 19200, 9600, 4800, 2400, 1200 Data Bits – 8, 7 Stop Bits – 1, 2 Parity – None, Odd, Even, Mark, Space
COM3	9600, 8 data bits, 1 stop bit, no parity Power on pin 9 (+5v) Disabled	Baud Rate – 38400, 19200, 9600, 4800, 2400, 1200 Data Bits – 8, 7 Stop Bits – 1, 2 Parity – None, Odd, Even, Mark, Space

Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Advanced Tab

Note: Scanner control panel options are based on the installed software version levels, driver and OS versions in the MX3-RFID. Your Scanner options may or may not be as described in this section. Contact your LXE representative to obtain current software and drivers for your mobile device.

Translate Control Codes



□ Translate Control Codes

□ Strip Leading 0 characters

□ Strip Trailing 0 characters

□ Prefix

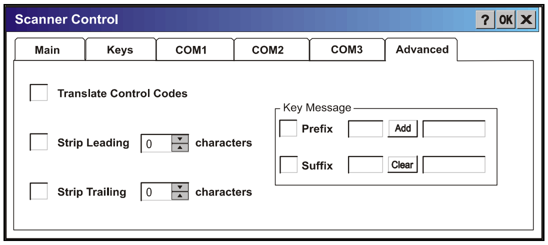
□ Suffix

Note: If your Advanced tab scanner panel has four button choices, as shown above, then when the Prefix/Suffix button is tapped, CTRL codes are passed through in Block mode.

If “Translate Control Codes” is checked, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

When “Translate Control Codes” is not checked and “Send Key Messages” is checked, CTRL codes are passed through in Block mode.

Strip Leading / Strip Trailing Characters



□ Translate Control Codes

□ Strip Leading 0 characters

□ Strip Trailing 0 characters

□ Prefix

□ Suffix

This feature, when enabled, strips the specified number of characters from a barcode, either from the beginning (leading) or at the end (trailing), or both.

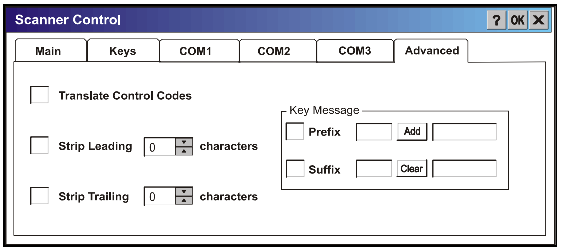
When this feature and the Add Prefix and / or Add Suffix fetaures are both enabled, the leading and trailing characters are stripped before the prefix or suffix is appended.

The configuration for stripping leading and trailing characters is specified independently. To enable, either or both of the checkboxes labeled Strip Leading and Strip Trailing must be checked. Then the number of characters to be stripped can be typed into the edit control or set using the spin control on the right of the edit control.

The maximum number of characters that can be stripped is 99 characters for each leading and trailing number of characters. When the Strip Leading and Strip Trailing checkboxes are blank (or disabled), the edit controls are disabled; however the last specified number of characters to strip is retained and dimmed.

When the number of characters to be stripped is greater than the number of characters in the barcode a good read beep is sounded but all barcode data is discarded.

Prefix / Suffix



□ Translate Control Codes

□ Strip Leading 0 characters

□ Strip Trailing 0 characters

□ Prefix

□ Suffix

If Add Prefix and / or Add Suffix are combined with Strip Leading and / or Strip Trailing, the leading and / or trailing characters are stripped before the prefix or suffix is added.

The mode for Prefix/Suffix feature is determined by the “Send Key Messages (WEDGE)” setting in the Main tab. When checked (enabled), the prefix/suffix feature is in *Key Message mode*. Key message mode sends the prefix, barcode, and suffix to the application with the focus as keystrokes. In Key message mode all keys on the keypad can be entered.

When the “Send Key Messages” is not checked, *Block mode* is enabled. Block mode allows ASCII characters (0x0 – 0x7F), plus backspace, tab, delete, return and escape. In Block mode the prefix/suffix data is added to the beginning and end of the buffered barcode data that can then be read by an application from the WDG: device.

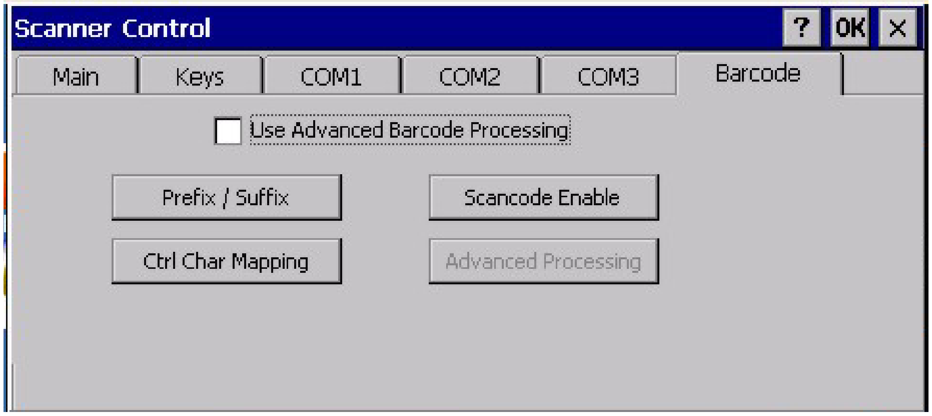
Up to 19 characters can be specified for the prefix and up to 19 characters can be specified for the suffix. The characters can be text or control characters, e.g. tab, carriage return. The characters can be entered into the prefix and suffix text boxes by typing from the keypad, entering the key’s hex equivalent, or entering in hat (^) encoded delimited (8-bit code table) notation.

- To enable the Prefix or Suffix processing, check the associated checkbox. When the box is checked, the edit controls to the right are enabled. Keys/characters are typed into the edit control following the checkbox.
- Selecting the Add button then adds the key to the associated list of keys in the read-only edit control to the right of the Add / Clear buttons. The keys are shown as comma-delimited strings.
- To erase the Prefix or Suffix, select the read-only edit control that contains the currently configured Prefix or Suffix and select the Clear button.
- The Add and Clear buttons function on the control that is selected when the button is pressed.
- Hex values can be entered by preceding the two digit hex value with ‘0x’. Control characters can also be entered using the ‘hat’ delimited notation, i.e. ^M for Carriage Return.
- All keypad keys can be entered by typing the key. Some keypad keys are only valid if in “Key Message” mode. For example, the Function Keys (F1, PF1) are only valid in “Key Message” mode.

See “Hat Encoding” and “Decimal-Hexadecimal Chart”.

Barcode Tab

Access: **Start | Settings | Control Panel | Scanner | Barcode tab**

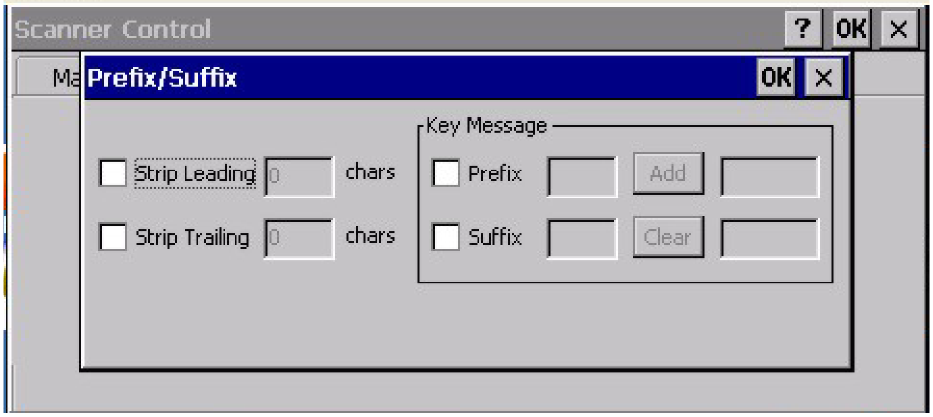


□ Use Advanced Barcode Processing

Figure 3-18 Barcode Tab

Prefix / Suffix

Note: Prefix / Suffix is only available when Use Advanced Barcode Processing is disabled.



□ Strip Leading 0 chars

□ Strip Trailing 0 chars

□ Prefix

□ Suffix

Figure 3-19 Barcode – Prefix / Suffix

Prefix/Suffix (and pre-existing data) is unavailable when *Use Advanced Barcode Processing* is enabled.

Strip Leading / Strip Trailing Characters

This feature, when enabled, strips the specified number of characters from a barcode, either from the beginning (leading) or at the end (trailing), or both.

When this feature and the Add Prefix and / or Add Suffix features are both enabled, the leading and trailing characters are stripped before the prefix or suffix is appended.

The configuration for stripping leading and trailing characters is specified independently. To enable, either or both of the checkboxes labeled Strip Leading and Strip Trailing must be checked. Then the number of characters to be stripped can be typed into the edit control or set using the spin control on the right of the edit control.

The maximum number of characters that can be stripped is 99 characters for each leading and trailing number of characters. When the Strip Leading and Strip Trailing checkboxes are blank (or disabled), the edit controls are disabled; however the last specified number of characters to strip is retained and dimmed.

When the number of characters to be stripped is greater than the number of characters in the barcode a good read beep is sounded but all barcode data is discarded.

Prefix / Suffix

If Add Prefix and / or Add Suffix are combined with Strip Leading and / or Strip Trailing, the leading and / or trailing characters are stripped before the prefix or suffix is added.

The mode for Prefix/Suffix feature is determined by the “Send Key Messages (WEDGE)” setting in the Main tab. When checked (enabled), the prefix/suffix feature is in *Key Message mode*. Key message mode sends the prefix, barcode, and suffix to the application with the focus as keystrokes. In Key message mode all keys on the keypad can be entered.

When the “Send Key Messages” is not checked, *Block mode* is enabled. Block mode allows ASCII characters (0x0 – 0x7F), plus backspace, tab, delete, return and escape. In Block mode the prefix/suffix data is added to the beginning and end of the buffered barcode data that can then be read by an application from the WDG: device.

Up to 19 characters can be specified for the prefix and up to 19 characters can be specified for the suffix. The characters can be text or control characters, e.g. tab, carriage return. The characters can be entered into the prefix and suffix text boxes by typing from the keypad, entering the key’s hex equivalent, or entering in hat (^) encoded delimited (8-bit code table) notation.

- To enable the Prefix or Suffix processing, check the associated checkbox. When the box is checked, the edit controls to the right are enabled. Keys/characters are typed into the edit control following the checkbox.
- Selecting the Add button then adds the key to the associated list of keys in the read-only edit control to the right of the Add / Clear buttons. The keys are shown as comma-delimited strings.
- To erase the Prefix or Suffix, select the read-only edit control that contains the currently configured Prefix or Suffix and select the Clear button.
- The Add and Clear buttons function on the control that is selected when the button is pressed.
- Hex values can be entered by preceding the two digit hex value with ‘0x’. Control characters can also be entered using the ‘hat’ delimited notation, i.e. ^M for Carriage Return.
- All keypad keys can be entered by typing the key. Some keypad keys are only valid if in “Key Message” mode. For example, the Function Keys (F1, PF1) are only valid in “Key Message” mode.

Interaction between Strip Leading/Trailing and Prefix/Suffix Settings

1. Replacements are not done on the Prefix and Suffix, only the barcode data, for both Block and Key Message mode. Control characters in the Prefix and Suffix are translated when Translate All is enabled.

2. Replacements are done on the barcode data and then characters are stripped for both Strip Leading and Strip Trailing features. As an example, suppose we have the following data and configuration:

   The barcode scanned begins with Group Separator (GS) followed by the character 'A'

   Group Separator is translated to 'GS'

   Strip Leading is set to 2

   In this case, the Group Separator is translated to 'GS' and then the 'GS' is stripped by the Strip Leading setting; rather than the Group Separator and 'A' being stripped.

3. If Translate All is enabled and replacements are assigned, the assigned replacements take precedence over the default one-to-one translation enabled by Translate all. For example if Translate All is enabled and Carriage Return is replaced by ^J, the value, 0x0d, in the barcode (prefix and suffix) are replaced with CTRL+Shift+J instead of CTRL+Shift+M keystrokes in Key Message mode.

4. Since the assigned replacements are applied before the Translate All is performed, if a control character is set to 'Ignore (drop)' by the assigned replacements, it is discarded before the Translate All processing is performed and is therefore not translated.

5. Since the assigned replacements are applied before the Translate All is performed, if a control character is set to text by the assigned replacements, the text is substituted for the control character. In this case, the control character would not be in the data processed by the Translate All feature.

6. If the application that is accessing the Barcode Wedge in Block mode, supports Hat encoded characters, like ^M, hat encoded characters can be assigned in the defined action and then interpreted by the receiving application by using the 'escape' format described above. The same is true for hex-encoded characters.

Ctrl Char Mapping

Access: | Settings | Control Panel | Scanner | Barcode tab

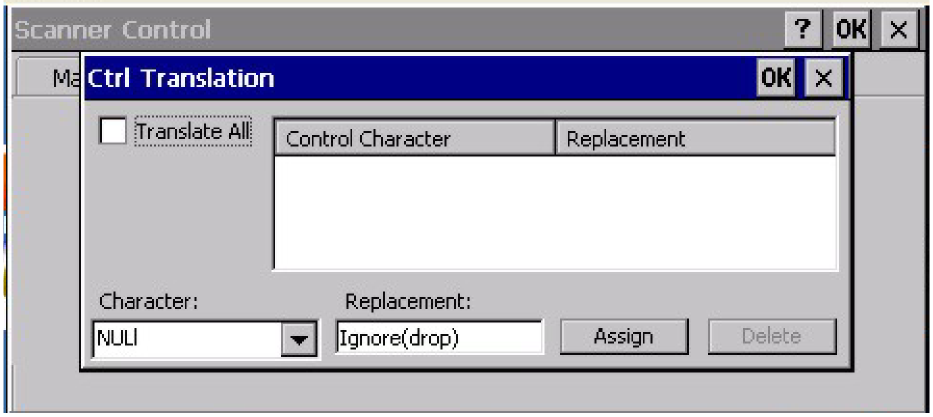


Figure 3-20 Barcode – Ctrl Translation

Note that Control Character Mapping is available regardless of the status of the *Use Advanced Barcode Processing* checkbox.

See “Hat Encoding” and “Decimal-Hexadecimal Chart”.

Translate All

If “Translate All” is checked, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

When “Translate All” is not checked and “Send Key Messages” is checked, CTRL codes are passed through in Block mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes in Key Message mode. If a control character is replaced by another control character, the replacement is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

For example, if ‘Carriage Return’ is replaced by Line Feed (by specifying ‘^J’ or ‘0x0A’) in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a.

The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

Translate All	This option is grayed unless the user has Key Message mode (on the Main tab) selected. In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent ‘control’ key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad). It does not replace control characters in the prefix and suffix. The assignments provided by this enhancement allow the user to override the one-to-one translation provided by Translate All.

Character This is a drop down combo box that contains the control character name. Refer to the table in “Assigned Replacements” for the list of control characters and their names. When a character name is selected from the combo box, the text ‘Ignore (drop)’ is shown and highlighted in the Replacement edit control. ‘Ignore (drop)’ is highlighted so the user can type a replacement if the control character is not being ignored. Once the user types into the Replacement edit control, reselecting the character form Character combo box redisplays the ‘Ignore (drop)’ default in the Replacement edit control.

Replacement The edit control where the user types the characters to be assigned as the replacement of the control character. Replacements for a control character are assigned by selecting the appropriate character from the Character combo box, typing the replacement in the Replacement edit control (according to the formats defined above) and then selecting Assign. The assigned replacement is then added to the list box above the Assign button.

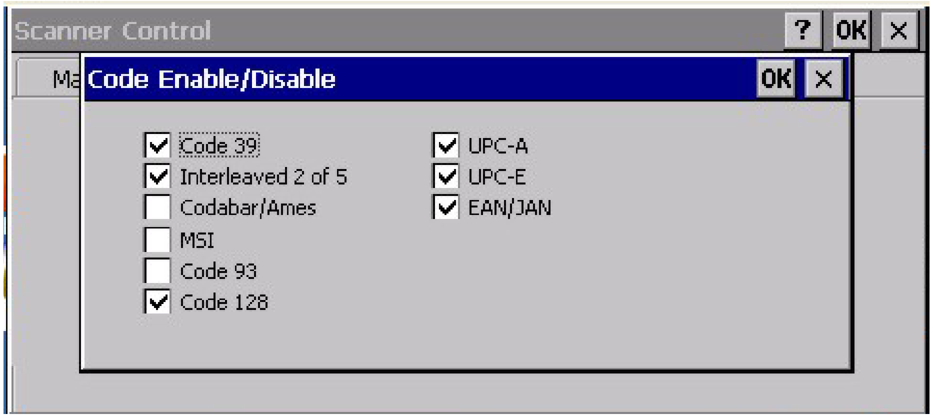
List Box The list box shows all user-defined control characters and their assigned replacements. All replacements are enclosed in single quotes to delimit white space that has been assigned.

Delete This button is grayed unless an entry in the list box is highlighted. When an entry (or entries) is highlighted, and Delete is selected, the highlighted material is deleted from the list box.

Scancode Enable

Access: | Settings | Control Panel | Scanner | Barcode tab

See the “Integrated Scanner Programming Guide”, section titled “Data Options” for full details on AIM Codes and Symbol Codes.



☑ Code 39
☑ Interleaved 2 of 5
□ Codabar/Ames
□ MSI
□ Code 93
☑ Code 128
☑ UPC-A
☑ UPC-E
☑ EAN/JAN

Figure 3-21 Barcode – Scancode Enable/Disable

Note that Scancode Enable is available regardless of the status of the *Use Advanced Barcode Processing* checkbox.

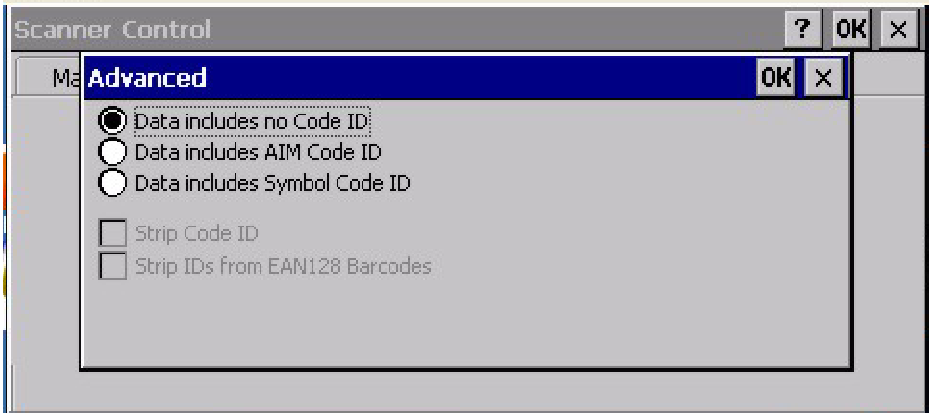
This panel displays a list of all barcode symbologies supported by the integrated barcode scanner. Barcodes are sent to the application just as they are received from the scanner and before the ‘Strip Leading / Trailing’ or ‘Append Prefix / Suffix’ features.

Advanced Processing

Access: | Settings | Control Panel | Scanner | Barcode tab

Note that the *Use Advanced Barcode Processing* checkbox must be enabled before Advanced Processing can occur.

See Also: The "Integrated Scanner Programming Guide", section titled "Data Options" for full details on AIM Code IDs and Symbol Code IDs.



● Data includes no Code ID

○ Data includes AIM Code ID

○ Data includes Symbol Code ID

□ Strip Code ID

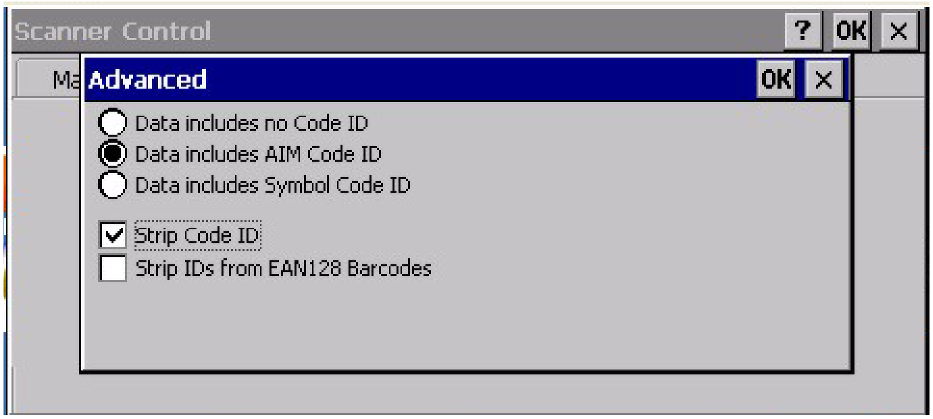
□ Strip IDs from EAN128 Barcodes

Figure 3-22 Barcode – Advanced Processing

No Code ID	Default. All symbology IDs are transmitted. This means that by default, all good scan barcodes are sent to the application just as they are received from the scanner, regardless of any possible symbology ID attached. The *Strip Code ID* radio button is unavailable when No Code ID is enabled.
AIM Code ID	Enabling the Strip Code ID checkbox ensures the 3-character AIM Code ID symbology is stripped off by the WEDGE before the barcode is made available to the application. Disable *Data includes Symbol Code ID* if the AIM Code ID parameter is enabled. When *Strip Code ID* is disabled (unchecked), the Code ID is included in the barcode data being matched.
Symbol Code ID	Enabling Strip Code ID ensures the 1-character Symbol Code ID symbology is stripped off by the WEDGE before the barcode is made available to the application. Disable *Data includes AIM Code ID* if the Symbol Code ID parameter is enabled. When *Strip Code ID* is disabled (unchecked), the Code ID is included in the barcode data being matched.

Strip Code ID

Enabling this parameter removes the number of characters (specified by AIM Code ID or Symbol Code ID radio button setting) before the barcode is sent to the application.



○ Data includes no Code ID
● Data includes AIM Code ID
○ Data includes Symbol Code ID

☑ Strip Code ID
□ Strip IDs from EAN128 Barcodes

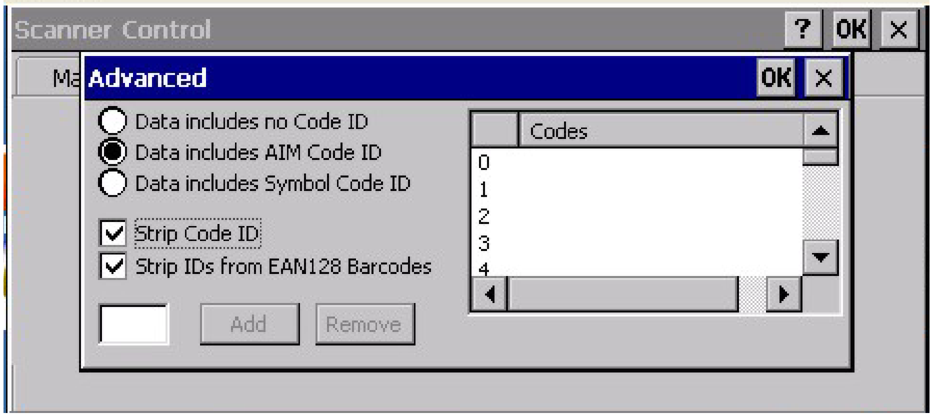
Figure 3-23 Barcode – Advanced Processing – Strip Code ID

This checkbox is unavailable when *Data includes no Code ID* radio button is enabled.

Strip Identifiers from EAN128 Barcodes

When *Strip Code ID* is disabled (unchecked), the AIM Code or Symbol Code ID is included in the barcode data being matched.

Scanned barcodes *are not matched* against the following parameters unless they are EAN128 barcodes. If the scan engine does not support EAN128 barcodes, or EAN128 barcodes have been disabled, the *Strip Identifiers from EAN128 Barcodes* function is not available.



○ Data includes no Code ID
● Data includes AIM Code ID
○ Data includes Symbol Code ID

☑ Strip Code ID
☑ Strip IDs from EAN128 Barcodes

Codes
0
1
2
3
4

Figure 3-24 Barcode – Advanced Processing – EAN128 Barcodes

The user specifies whether the barcodes have an AIM Code ID (3 characters) or a Symbol Code ID (1 character). They also specify whether the AIM or Symbol Code ID will be stripped or passed through to the Codes match, **as long as the barcode is an EAN128 barcode**.

Adding Codes to the Match List for EAN128 Barcodes

The first elements of an EAN128 barcode are matched against the entries in the Match Code list, in the order entered in the list. For example, if the match code list contains *Item 0 ABC, Item 1 C* and *Item 2 AB* in that order, the *AB* has no effect. When a match is found (e.g. Code ID *A* was matched by *Item 0 ABC* and the process terminated) or when the end of the list is reached, processing terminates.

Up to 20 Codes (up to 16 characters each) can be added to the Match list. The characters can be text or control characters, e.g. tab, carriage return. The characters can be entered into the Match Code List text box by typing from the keypad, entering the key's hex equivalent, or entering in hat (^) encoded delimited (8-bit code table) notation.

- Keys/characters are typed into the lower left text box.
- To add a match code, move the cursor to the lower left text box. Add the characters to the box and select the Add button to place the new Match Code in the List Box.
- To edit a match code, highlight the match code in the List Box and double-click. The match code text is moved to the lower left text box. Make changes to the copied match code and select the Add button.
- To delete a match code, highlight the code in the List Box and select the Remove button. The match code is deleted from the list.
- After adding, editing or removing match codes, perform the Suspend/Resume function to store your changes in the registry.
- Hex values can be entered by preceding the two digit hex value with '0x'. Control characters can also be entered using the 'hat' delimited notation, i.e. ^M for Carriage Return. See "Hat Encoding" and "Decimal-Hexadecimal Chart" at the end of Chapter 5 "MX3-RFID".
- All keypad keys can be entered by typing the key.

Note: No matching is done for barcodes using this option if they are not EAN128 barcodes.

Storage Manager

Access: Start | Settings | Control Panel | Storage Manager

Installed storage devices are listed by device name in the dropdown box. To view information about the disk or perform store operations, select a device from the list.

On-line help is available for this option.

- Topics available are:
  - Manage storage devices
  - Manage disk partitions
  - Creating a new partition
  - Advanced partition features

LXE recommends **caution** when formatting or dismounting storage devices and when creating new partitions or deleting partitions on the storage device.

Note: Contact LXE Customer Support prior to using management functions on the internal ATA card.

Stylus

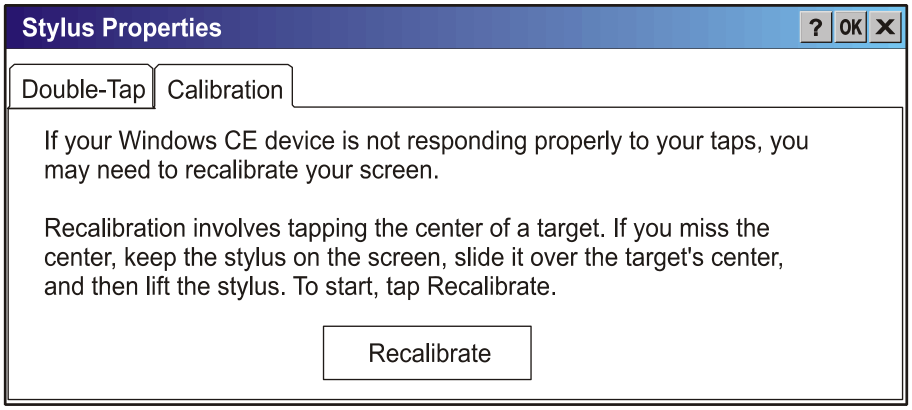
Access: Start | Settings | Control Panel | Stylus

Set double-tap sensitivity properties and/or calibrate the touch panel.

Double Tap

Follow the instructions on the screen and tap the OK box to save the changes. The changes take effect immediately.

Calibration

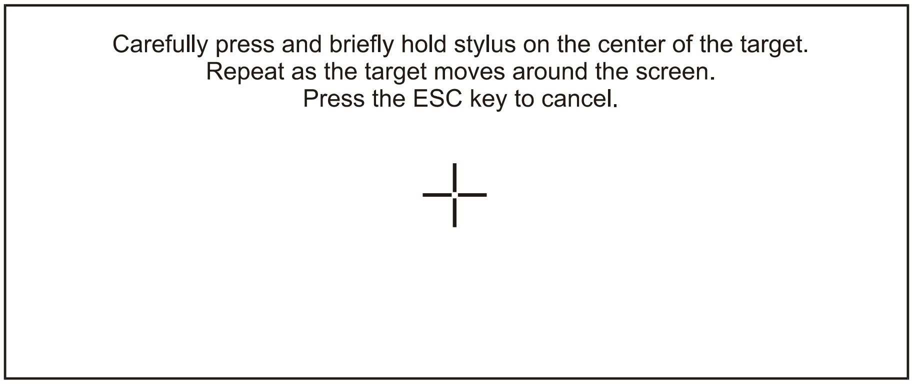


Stylus Properties

If your Windows CE device is not responding properly to your taps, you may need to recalibrate your screen.

Recalibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus. To start, tap Recalibrate.

Figure 3-25 Stylus Properties / Recalibration Start



Carefully press and briefly hold stylus on the center of the target.
Repeat as the target moves around the screen.
Press the ESC key to cancel.

Figure 3-26 Stylus Properties / Recalibration

System

Access: Start | Settings | Control Panel | System Icon

Review System and Computer data and revision levels. Adjust Storage and Program memory settings.

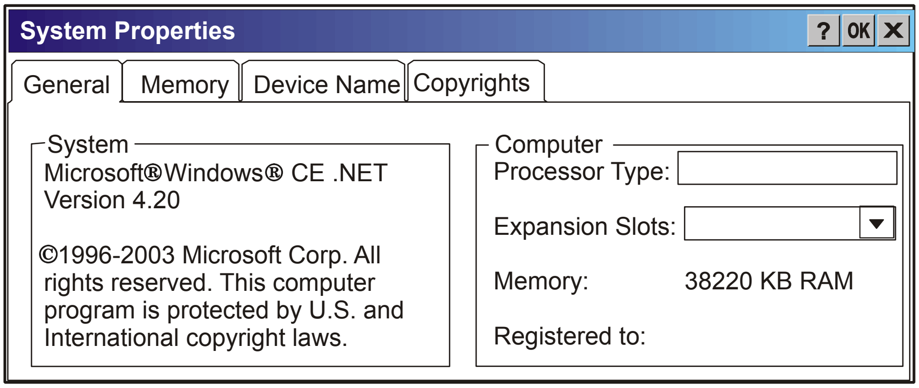
Factory Default Settings	
General	N/A
Memory	1/3 storage, 2/3 programs.
Device Name	MX3X001
Device Description	LXE_MX3X
Copyrights	N/A

Persist RAM Base Files

"Desktop"
"Favorites"
"Fonts"
"Help"
"Programs"

If you create a directory or directories with the above listed names in the "\System" folder (which is on the CF ATA card) and place your files in those directories, the Launch utility will automatically copy all of the files in these directories to the respective RAM base folders every time upon warm boot.

General



System
Microsoft®Windows® CE .NET
Version 4.20

©1996-2003 Microsoft Corp. All rights reserved. This computer program is protected by U.S. and International copyright laws.

Computer
Processor Type:
Expansion Slots:
Memory: 38220 KB RAM
Registered to:

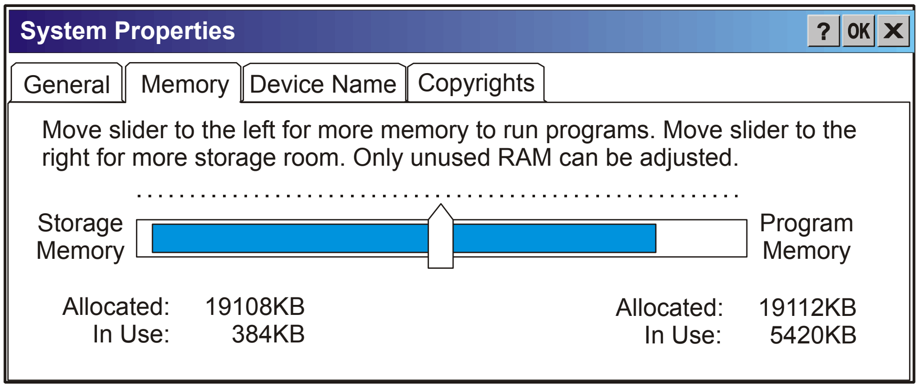
Figure 3-27 System / General tab

System: This screen is presented for information only. The System parameters cannot be changed by the user.

Computer: The processor type is listed. The type cannot be changed by the user. The name of the installed wireless card is listed in the dropdown list. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

Memory sizes given do not include memory used up by the operating system. Hence, a system with 64 MB may only report 35 MB memory, since 29 MB is used up by the Windows CE .NET operating system. This is actual DRAM memory, and does not include internal flash or the internal ATA card used for storage.

Memory



Move slider to the left for more memory to run programs. Move slider to the right for more storage room. Only unused RAM can be adjusted.

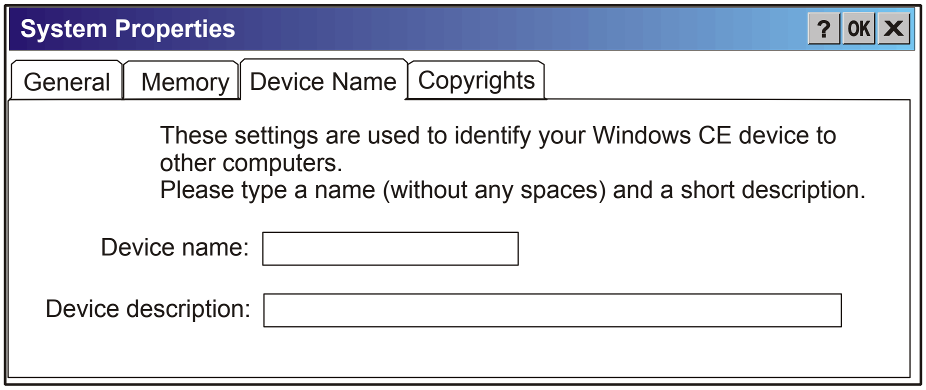
Allocated: 19108KB
In Use: 384KB

Allocated: 19112KB
In Use: 5420KB

Figure 3-28 System / Memory

Move the slider to allocate more memory for programs or storage. If there isn’t enough space for a file, increase the amount of storage memory. If the mobile device is running slowly, try increasing the amount of program memory. Adjust the settings and tap the OK box to save the changes. The changes take effect immediately.

Device Name



These settings are used to identify your Windows CE device to other computers.
Please type a name (without any spaces) and a short description.

Device name:

Device description:

Figure 3-29 System / Device Name

The device name and description can be changed. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. The changes take effect immediately.

Copyrights

This screen is presented for information only. The Copyrights information cannot be changed by the user.

Volume and Sounds

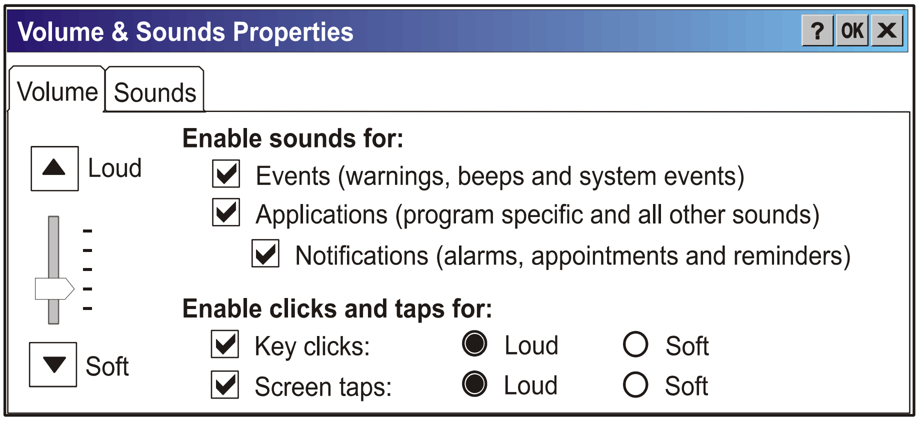
Access: **Start | Settings | Control Panel | Volume & Sounds Icon**

Set volume parameters and assign sound wav files to CE .NET events.

Note: Control Panel parameters established in Display Properties, Power Properties and Volume & Sounds Properties remain in effect during RFID configuration and the resulting read functions.

Factory Default Settings	
Volume	
Events	Enabled
Application	Enabled
Notifications	Enabled
Volume	Middle of Bar
Key click	Loud
Screen tap	Loud
Sounds	
Scheme	LOUD!

Follow the instructions on the screen and tap the OK box to save the changes. The changes take effect immediately.



Enable sounds for:

☑ Events (warnings, beeps and system events)

☑ Applications (program specific and all other sounds)

☑ Notifications (alarms, appointments and reminders)

Enable clicks and taps for:

☑ Key clicks: ● Loud ○ Soft

☑ Screen taps: ● Loud ○ Soft

Figure 3-30 Volume and Sounds

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user’s choice. By default a good scan sound on the mobile device is a single 2700 Hz beep, and a bad scan sound is a double beep.

Utilities

These utilities are pre-loaded by LXE.

LAUNCH.EXE

All applications to be installed into persistent memory are normally in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and need to be copied to the mobile device using an internal ATA card or from a PC using ActiveSync. The CAB files are loaded into the folder **System**, which is the internal ATA drive.

Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup. The CAB file can update the registry as desired and cause the unpacked file(s) to be placed in the appropriate location.

The registry information needed is under the key *HKEY_LOCAL_MACHINE \ SOFTWARE \ LXE \ Persist*, as follows. The main subkey is any text, and is a description of the file. Then 3 values are added:

FileName is the name of the CAB file, with the path (usually \System)
Installed is a DWORD value of 0, which changes to 1 once auto-launch installs the file
FileCheck is the name of a file to look for to determine if the CAB file is installed.

The value in FileCheck is the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

3 optional fields are also added: **Order**, **Delay**, and **PCMCIA**. These are all DWORD fields, described below.

The auto-launch process goes as follows. The launch utility opens the registry database and reads the list of CAB files to auto-launch. First it looks for **FileName** to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the **Installed** flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it. If the **Installed** flag is set, auto-launch looks for the **FileCheck** file. If it is present, the CAB file is installed, and that registry entry is complete. If the **FileCheck** file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file. Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.

To force execution every time (for example, for **AUTOEXEC.BAT**), use a **FileCheck** of **"dummy"**, which will never be found, forcing the item to execute.

For persist keys specifying **.EXE** or **.BAT** files, the executing process will be started, and then **Launch** will continue, leaving the loading process to run independently. For other persist keys (including **.CAB** files), **Launch** will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.

The **Order** field is used to force a sequence of events; **Order=0** is first, and **Order=99** is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence. Note: If the order of loading is not critical, it may be easier to use the \System\Startup folder instead; see below (only on **.01D** or newer images).

The **Delay** field is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to **0** if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.

The **PCMCIA** field is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the "Unidentified PCMCIA Slot" dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the **PCMCIA** field is a

DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of **0** means the slot is not powered on. The default values for the default radio drivers (listed below) is **1**, meaning one second elapses between the CAB file loading and the slot powering up.

Note that the auto-launch process can also launch batch files (***.BAT**), executable files (***.EXE**), registry setting files (***.REG**), or sound files (***.WAV**). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Registry information is already in the default image for the following [1]:

```
        ; Summit Client
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Summit Radio]
        "FileName"="\SYSTEM\SUMMIT.CAB"
        "Installed"=dword:1
        "FileCheck"="\WINDOWS\SDCCFG10G.DLL"
        "Order"=dword:02
        "Delay"=dword:0
        "PCMCIA"=dword:1

        ; Cisco Client
 [HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Cisco Radio]
        "FileName"="\SYSTEM\CISCO.CAB"
        "FileCheck"="\WINDOWS\CISCO.DLL"
        “Order”=dword:01
        “PCMCIA”=dword:1

        ; this key installs RFID drivers/default values from the CAB file
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFID]
        "FileName"="\WINDOWS\RFID.CAB"
        "FileCheck"="\WINDOWS\RFID_WDG.DLL"
        “Order”=dword:0C

        ; this key installs RFTERM from the CAB file
 [HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\LXE TE]
        "FileName"="\SYSTEM\RFTERM.CAB"
        "FileCheck"="\WINDOWS\LXE\RFTERM.EXE"
        “Order”=dword:10

        ; this key installs JAVA
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Java]
        "FileName"="\SYSTEM\JEODE.CAB"
        "FileCheck"="\WINDOWS\EVM.EXE"
        “Order”=dword:30

        ; this key runs RFTERM as a startup app
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\RFTERM]
        "FileName"="\WINDOWS\LXE\RFTERM.EXE"
        "FileCheck"="dummy"
        “Order”=dword:40
```

[1] CAB files for options not purchased are not loaded e.g. JAVA or RFID. If a CAB file is missing, please contact your LXE Representative.

```
        ; Autoexec
 [HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AUTOEXEC]
        "FileName"="\SYSTEM\AUTOEXEC.BAT"
        "FileCheck"="dummy"
        “Order”=dword:50

        ; Avalanche
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\Avalanche]
        "FileName"="\SYSTEM\LXEAVA.CAB"
        "FileCheck"="\SYSTEM\AVALANCHE\MODEL.DAT"
        "Order"=dword:4
        "Installed"=dword:0
        "PCMCIA"=dword:0
        "Delay"=dword:0

        ; Avalanche
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\AvaLaunch]
        "FileName"="\SYSTEM\AVALANCHE\AVAINIT.EXE"
        "FileCheck"="dummy"
        “Order”=dword:5
        "Delay"=dword:0
        "PCMCIA"=dword:0
        "Installed"=dword:0
```

When you are installing your custom CAB file to the mobile device’s operating sytem, refer to the default image segments that are commented with “… RFTERM …” to see the expected Registry format.

One special key is included to force the system folders (Desktop, Fonts, Programs, etc.) to copy from the internal ATA card (**\System**) to the **\Windows** directory. This is implemented as a persist key so the sequence of startup events can be controlled (especially for AppLock). The filename is a special internal trigger for the Launch utility, to activate the **CopyFolders** function. *DO NOT EDIT OR ALTER THIS KEY, OR IT MAY NO LONGER FUNCTION.* You may however change the **Order** or **Delay** values if necessary for a particular startup sequence.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\LXE\Persist\COPYFOLDERS]
        "FileName"="COPYFOLDERS"
        "FileCheck"=""
        “Order”=dword:0F
```

To have files (CAB, EXE, REG, or WAV files) loaded on startup, when sequence of execution is not important, you can put these files in the \System\Startup folder (on the internal ATA card). This is parsed by the Launch utility, and these programs are started or executed. Note that this only works on images from **.01D** and newer.

REGEDIT.EXE

Before using REGEDIT.EXE, please refer to commercially available Microsoft Windows manuals. For example, Microsoft Windows Registry Guide, Second edition.

The Registry Editor allows viewing, searching for items and changing settings in the registry. The registry contains information about how the mobile device runs. LXE recommends **caution** when inspecting and editing the Registry as making incorrect changes can damage the mobile device operating system. LXE recommends making a backup copy of the registry before viewing or carefully making changes to the registry.

REGLOAD.EXE

Double-tapping a registry settings file (e.g. REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

WARMBOOT.EXE

Double tap this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double-tapping a sound file (e.g. WAV) causes WavPlay to open the file and run it in the background.

Enabling GrabTime

The MX3-RFID has a GrabTime utility which can automatically synchronize the MX3-RFID with a time server (via an Internet connection) at boot up.

By default, using GrabTime for time synchronization at boot up is Off. Grabtime can be run at any time (even when Off at boot up) using the Sync button on the Date/Time control panel.

To enable GrabTime to run automatically at boot up, run \Windows\tmsync.reg and perform a warmboot. For more detail, see “LAUNCH.EXE”, earlier in this chapter.

Note: This utility affects the behavior of GrabTime at warmboot. After a coldboot, GrabTime is disabled.

Disabling the Touchscreen

To disable the touchscreen, run \Windows\TouchDisable.reg and perform a warm reboot.

To enable the touchscreen, run \Windows\TouchEnable.reg and perform a warm reboot.

Note: These utilities affect the behavior of the touchscreen on warmboot. After a coldboot, the touchscreen is enabled. Enable this option with caution.

Troubleshooting

Touchscreen is not accepting stylus taps or need recalibration.	Press <Ctrl>+<Esc> to force the Start Menu to appear. Use the tab, backtab and cursor keys to move the cursor from element to element.

Configuring CapsLock Behavior

To set CapsLock status to On after a warmboot, run \Windows\CapsLockOn.reg and perform a warmboot.

To set CapsLock status to Off after a warmboot, run \Windows\CapsLockOff.reg and perform a warmboot.

Note: Setting CapsLock to On using this method does not display the CapsLock icon in the Windows CE taskbar. The current status of CapsLock can be changed with the CAPS key, however this method does not change CapsLock behavior upon reboot.

Note: These utilities affect the behavior of the CapsLock on warmboot. After a coldboot, CapsLock is disabled.

Configuring IPv6

By default, IPv6 is enabled and an IPv6 broadcast message is sent on power up.

To disable IPv6, run \Windows\ipv6Disable.reg and perform a warmboot.

To enable IPv6, run \Windows\ipv6Enable.reg and perform a warmboot.

Note: These utilities affect the behavior of IPv6 on warmboot. After a coldboot, IPv6 is enabled.

Command-line Utility

Command line utilities can be executed by Start | Run | [program name].

COLDBOOT.EXE

Command line utility which performs a cold boot (all data in RAM is erased). The command is not case-sensitive.

Passwords are lost upon cold boot. If a password is set, that password must be entered to begin the cold boot power cycle process.

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap Start | Run | then type prtscrn and tap OK, or press Enter. There is a 10 second delay before the screen print is made. The device beeps and screen captured file (scr*nnnnn*.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

Reflash the Mobile Device

Note: When reflashing, LXE recommends using a Compact Flash card that is greater than 64MB. Files to be loaded on the CF card are: NK.BIN, EBOOT.NB0, XSCALE.BIT

Caution ⚠	Make sure the backup battery has been fully charged before beginning the reflash procedure. Depleting the backup battery during the reflash process can result in corrupted files. LXE also recommends installing a fully charged main battery before beginning the reflash procedure.

Requirement: A screwdriver (not supplied by LXE)

Preparation

- LXE recommends that installation of the CF card be performed on a clean, well-lit surface.
- Remove the screws on the endcap and slide the endcap to the side, being very careful not to disconnect the ribbon cables, damage the leads to the external power jack, the headphone jack or the antenna. The antenna may be taped to the endcap so great care must be taken when loosening the endcap.
- Carefully remove or loosen all cables to an existing CF card. Remove the CF card.

How To : Reflash using Keypress Method

1. Place the compact flash card with new image files on it in the right hand slot.
2. Double-tap **My Computer**, then **Storage Card** folder.
3. Select NK.BIN, EBOOT.NB0, XSCALE.BIT. Select **Edit | Copy**.
4. Tap **Back Arrow**. Double-tap **System Folder**.
5. Select **Edit | Paste**. When asked “Overwrite ?”, tap **Yes to All**.
6. When the copy process finishes, remove the CF card.
7. Select **Start | Run** and type **Coldboot**.
8. Before the splash screen appears, press and hold down the <A> key. Continue to hold it down until the displays shows “Writing to boot flash”.

   Note: If you do not press and hold the <A> key quickly enough, the display shows “Loading OS Image”. Remove the main battery for 2 seconds, re-insert the battery and press the Power button. Press and hold the <A> key again.

9. The mobile device will automatically reboot after flashing the bootloader. “Loading OS Image” is displayed on the screen and when the new OS finishes loading, all software upgrades are complete.
10. Replace the endcap, being careful not to pinch any leads or cables. The touchscreen will need to be re-calibrated.

Once the bootloader is loaded and the files are copied onto the internal ATA drive, you can reflash the bootloader at any time by rebooting the MX3-RFID, and holding down the <A> key on the keypad before the splash screen appears.

Wait until the splash screen displays “Writing new bootloader”, and you can release the <A> key. When complete (3-5 seconds), the MX3-RFID will reboot and startup with the new bootloader again.

How To: Reflash using TAG file Method

1. Place the compact flash card with new image files on it in the right hand slot.
2. Double-tap **My Computer**, then **Storage Card** folder.
3. Select NK.BIN, EBOOT.NB0, XSCALE.BIT. Select **Edit | Copy**.
4. Tap **Back Arrow**. Double-tap **\System** folder.
5. Select **Edit | Paste**. When asked “Overwrite ?”, tap **Yes to All**.
6. Additionally a REFLASH.TAG file is needed to trigger the reflash. This file can be created on the MX3-RFID or copied to it along with the system files. The contents of the file are unimportant; but the file must be named REFLASH.TAG and it must be in the **\System** folder with the new system load.
7. When the copy process finishes, remove the CF card.
8. Select **Start | Run** and type **Coldboot**.
9. When booting, the MX3-RFID looks for a file named REFLASH.TAG in the \System folder.
   - When this file is encountered, the MX3-RFID loads a new bootloader image (eboot.nb0) into the boot flash. The tag file is deleted and the MX3-RFID is rebooted to begin using the new boot loader.
   - If EBOOT detects this file, a re-flash sequence is initiated. The .TAG file is deleted and the MX3-RFID reboots.
   - If EBOOT detects the REFLASH.TAG file and there is no .nb0 file it does not re-flash and deletes the REFLASH.TAG file to prevent an endless cycle.
10. The mobile device automatically reboots after flashing the bootloader. “Loading OS Image” is displayed on the screen and when the new OS finishes loading, all software upgrades are complete
11. Replace the endcap, being careful not to pinch any leads or cables. The touchscreen will need to be re-calibrated.

Clearing Persistent Storage

Cold boot sets all registry settings back to LXE factory defaults. No other clearing is available or necessary.

API Calls

See Also: LXE CE API Programming Guide E-SW-WINAPIPG

The LXE CE API Programming Guide documents only the LXE-specific API calls for the mobile device. It is intended as an addition to the standard Microsoft Windows CE API documentation. Details of many of the calls in the LXE guide may be found in Microsoft's documentation.

The APIs documented in the programming guide are included in the file LXEAPI.ZIP, which is in the standard Windows CE image on the mobile device.

For ease of software development, the files LXEAPI.H and LXEAPI.LIB are available on the accessories CD, which are the C/C++ include files and the link library for the DLL, respectively. Note that this DLL is installed in mobile device images with a version number of 1.2 or higher (as displayed on the screen during bootup).

A full SDK is now included for Microsoft Embedded Visual C++ 4.0 (which is available free on the Microsoft website).

See Also: "RFID Driver APIs".

RFID Driver APIs

For the development of applications to execute locally on the MX3-RFID device, API support for the functions described supplement the current MX3X APIs documented in the "LXE CE API Programming Guide" (available on the LXE Manuals CD or the LXE ServicePass website).

For ease of software development, the library file, RFIDAPI.LIB, and two header files, RFIDAPI.H and LXERFID.H, are available on the MX3X SDK CD (see "Accessories"). Contact your LXE representative for the MX3X SDK Kit availability.

The following operations take place when a user presses a scan button mapped to an RFID Read command.

1. Scanner Wedge catches a Keyboard Event and determines that the key pressed is mapped to an "RFID Read" operation.
2. RFID Driver executes the READ command. Based on the "Tag Types to Read" setting (set through the LXE RFID Configuration Utility), the command calls either of the following: TAG_0_READ, TAG_1_READ, or both TAG_0_READ and TAG_1_READ.
3. The Reader receives an API call, performs an appropriate read, and returns tag data to the RFID Driver.
4. Based on the "Reader Output" settings (set through the LXE RFID Configuration Utility), the RFID Driver formats the tag data with a preamble, postamble, and separators.
5. RFID Driver populates the Keyboard Buffer with the formatted data output.

Formatted data is displayed in the foreground application window.

System Commands

NO_CHG	No Commands, RFIDchange (the system mode is not changed). Used to retrieve firmware version.

Class 0 Commands

KILL	*Kill Class 0 tag (not supported)*
SET	Set read parameters (RF power level and Modulation depth)
READ	Read Class 0 tag IDs using parameters set by TAG_0_SET

Class 1 Commands

KILL	*Kill Class 1 tag (not supported)*
SET	Set read parameters (RF power level and Modulation depth)
READ	Read Class 1 tag IDs using parameters set by TAG_1_SET
READ_ALL	Read Class 1 tag IDs using parameters set by TAG_1_SET. (Unlike READ, this command does not filter out tags that do not conform to EPC tag data standards.)
PROGRAM_ID	All Class 1 tags receiving this command will program the specified tag ID in memory
VERIFY_ID	All tags receiving this command will reply with their CRC, followed by their entire ID code, followed by their Password. A tag that has successfully executed the LOCK_ID command ignores the VERIFY_ID command.
LOCK_ID	This command prevents any further modification of the tag ID, CRC, and Password.
ERASE_ID	This command sets all bits of the tag ID, CRC, and Password to ‘0’. A tag that has successfully executed the LOCK_ID command ignores the ERASE_ID command
WRITE	Performs/combines Program_ID and Lock_ID

Gen 2 Commands

Kill	Kill Class 1 tag.
SET	Set read parameters (RF power level and Modulation depth).
READ	Read Class 1 tag IDS using parameters et by TAG_1_SET.
PROGRAM_ID	All Class 1 tags receiving this command will program the specified tag ID in memory.
LOCK_ID	This command prevents any further modification of the tag ID, CRC, and Password.

Data Format Commands

MASK_DEFINE Allows definition of a set of six masks, each containing a Field Name, Offset, and Mask Value. Updates registry values.

MASK_READ Reads Class 0 tags or Class 1 tags depending on the value passed in for TAG_TYPE parameter. Allows a maximum of six masks as an Input.

SET_PREAMBLE Sets preamble for the output of all read commands (TAG_0_READ, TAG_1_READ, and MASK_READ)

SET_POSTAMBLE Sets postamble for the output of all read commands (TAG_0_READ, TAG_1_READ, and MASK_READ)

SET_SEPARATOR Sets tag separator for the output of all read commands (TAG_0_READ, TAG_1_READ, and MASK_READ)

Power Commands

READER_POWER_TIMEOUT Sets the timeout for the Reader Power Management to kick in. When the driver is inactive for the specified time, it puts the reader into "Disabled" mode to conserve power.

Reader Feedback Commands

NOTIFY_READ_SUCCESS Turn ON/OFF beep on a read operation that results in one or more tags read. See table below.

NOTIFY_READER_ON Turn ON/OFF buzz on a read operation that does not produce a beep. See table below.

Settings	Read Result	
	Tag(s) Read	No Tags Read
Beep On / Buzz On	Beep	Buzz
Beep On / Buzz Off	Beep	No sound
Beep Off / Buzz On	Buzz	Buzz
Beep Off / Buzz Off	No sound	No sound

LXE RFID Get Data Commands

Get_Data Returns the tag data acquired in the last RFID Read. WM_LXE_RFIDFULL message indicates that RFID Read is complete.

WM_LXE_RFIDFULL Indicates that the RFID Read is complete.

Hat Encoding

The MX3-RFID supports only 7-bit hat encoding which means only ^@ through ^_ (underscore) are supported.

Desired ASCII	Hex Value	Hat Encoded
NUL	00	^@
SOH	01	^A
STX	02	^B
ETX	03	^C
EOT	04	^D
ENQ	05	^E
ACK	06	^F
BEL	07	^G
BS	08	^H
HT	09	^I
LF	0A	^J
VT	0B	^K
FF	0C	^L
CR	0D	^M
SO	0E	^N
SI	0F	^O
DLE	10	^P
DC1 (XON)	11	^Q
DC2	12	^R
DC3 (XOFF)	13	^S
DC4	14	^T
NAK	15	^U
SYN	16	^V
ETB	17	^W
CAN	18	^X
EM	19	^Y
SUB	1A	^Z
ESC	1B	^[
FS	1C	^\\
GS	1D	^]
RS	1E	^^
US	1F	^_ (Underscore)
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~”
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~’
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)

Figure 3-31 Hat Encoded Characters Hex 00 through AD

Desired ASCII	Hex Value	Hat Encoded
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z
Û	DB	~[
Ü	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

Figure 3-32 Hat Encoded Characters Hex AE through FF

Decimal - Hexadecimal Chart

0	0x00	40	0x28	80	0x50	120	0x78
1	0x01	41	0x29	81	0x51	121	0x79
2	0x02	42	0x2A	82	0x52	122	0x7A
3	0x03	43	0x2B	83	0x53	123	0x7B
4	0x04	44	0x2C	84	0x54	124	0x7C
5	0x05	45	0x2D	85	0x55	125	0x7D
6	0x06	46	0x2E	86	0x56	126	0x7E
7	0x07	47	0x2F	87	0x57	127	0x7F
8	0x08	48	0x30	88	0x58	128	0x80
9	0x09	49	0x31	89	0x59	129	0x81
10	0x0A	50	0x32	90	0x5A	130	0x82
11	0x0B	51	0x33	91	0x5B	131	0x83
12	0x0C	52	0x34	92	0x5C	132	0x84
13	0x0D	53	0x35	93	0x5D	133	0x85
14	0x0E	54	0x36	94	0x5E	134	0x86
15	0x0F	55	0x37	95	0x5F	135	0x87
16	0x10	56	0x38	96	0x60	136	0x88
17	0x11	57	0x39	97	0x61	137	0x89
18	0x12	58	0x3A	98	0x62	138	0x8A
19	0x13	59	0x3B	99	0x63	139	0x8B
20	0x14	60	0x3C	100	0x64	140	0x8C
21	0x15	61	0x3D	101	0x65	141	0x8D
22	0x16	62	0x3E	102	0x66	142	0x8E
23	0x17	63	0x3F	103	0x67	143	0x8F
24	0x18	64	0x40	104	0x68	144	0x90
25	0x19	65	0x41	105	0x69	145	0x91
26	0x1A	66	0x42	106	0x6A	146	0x92
27	0x1B	67	0x43	107	0x6B	147	0x93
28	0x1C	68	0x44	108	0x6C	148	0x94
29	0x1D	69	0x45	109	0x6D	149	0x95
30	0x1E	70	0x46	110	0x6E	150	0x96
31	0x1F	71	0x47	111	0x6F	151	0x97
32	0x20	72	0x48	112	0x70	152	0x98
33	0x21	73	0x49	113	0x71	153	0x99
34	0x22	74	0x4A	114	0x72	154	0x9A
35	0x23	75	0x4B	115	0x73	155	0x9B
36	0x24	76	0x4C	116	0x74	156	0x9C
37	0x25	77	0x4D	117	0x75	157	0x9D
38	0x26	78	0x4E	118	0x76	158	0x9E
39	0x27	79	0x4F	119	0x77	159	0x9F

Figure 3-33 Decimal - Hexadecimal Chart (0 to 159 Decimal)

160	0xA0	200	0xC8	240	0xF0
161	0xA1	201	0xC9	241	0xF1
162	0xA2	202	0xCA	242	0xF2
163	0xA3	203	0xCB	243	0xF3
164	0xA4	204	0xCC	244	0xF4
165	0xA5	205	0xCD	245	0xF5
166	0xA6	206	0xCE	246	0xF6
167	0xA7	207	0xCF	247	0xF7
168	0xA8	208	0xD0	248	0xF8
169	0xA9	209	0xD1	249	0xF9
170	0xAA	210	0xD2	250	0xFA
171	0xAB	211	0xD3	251	0xFB
172	0xAC	212	0xD4	252	0xFC
173	0xAD	213	0xD5	253	0xFD
174	0xAE	214	0xD6	254	0xFE
175	0xAF	215	0xD7	255	0xFF
176	0xB0	216	0xD8		
177	0xB1	217	0xD9		
178	0xB2	218	0xDA		
179	0xB3	219	0xDB		
180	0xB4	220	0xDC		
181	0xB5	221	0xDD		
182	0xB6	222	0xDE		
183	0xB7	223	0xDF		
184	0xB8	224	0xE0		
185	0xB9	225	0xE1		
186	0xBA	226	0xE2		
187	0xBB	227	0xE3		
188	0xBC	228	0xE4		
189	0xBD	229	0xE5		
190	0xBE	230	0xE6		
191	0xBF	231	0xE7		
192	0xC0	232	0xE8		
193	0xC1	233	0xE9		
194	0xC2	234	0xEA		
195	0xC3	235	0xEB		
196	0xC4	236	0xEC		
197	0xC5	237	0xED		
198	0xC6	238	0xEE		
199	0xC7	239	0xEF		

Figure 3-34 Decimal - Hexadecimal Chart (160 to 255 Decimal)

Chapter 4 Wireless Network Configuration

Introduction

The MX3-RFID offers a choice of Cisco or Summit clients. The radios are 802.11b/g radios. The radio can be configured for no encryption, WEP encryption or WPA security protocols.

Certificates are necessary for many of the WPA authentications. Please refer to the “Certificates” section at the end of this chapter for more information on generating and installing certificates.

Please refer to the table below for the security options supported for each radio type.

Security Options Supported	Type	
	Summit Client	**Cisco Client**
None	Yes	Yes
WEP	Yes	Yes
LEAP	Yes	Yes
WPA-PSK	Yes	Yes
WPA/LEAP	Yes	Yes
PEAP-MSCHAP	Yes	Yes
PEAP-GTC	No	Yes
EAP-TLS	No	Yes

Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys
- The Summit profile settings for *Auth Type*, *EAP Type* and *Encryption* depend on the security option chosen.

📖	Please refer to the “LXE Security Primer” to prepare the Authentication Server and Access Point for MX3-RFID communication. It is available on the LXE Manuals CD and the LXE ServicePass website.
Date/Time	It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Summit Client Configuration

Summit Client Utility Icon

Start the Summit Client configuration by tapping the Summit Client Utility icon on the desktop. You can also start the Summit Client utility by tapping **Start | Programs | Summit | SCU**.

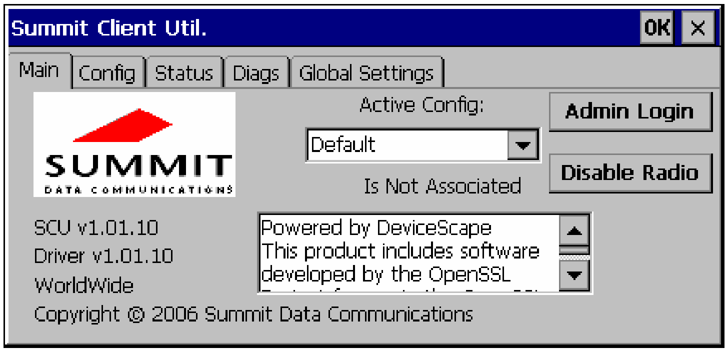
All LXE mobile devices with a Summit Client ship with this software revision or greater. To identify the software revision, tap the "About" icon in **Start | Settings | Control Panel**.

The radio is an 802.11g radio, capable of both 802.11b and 802.11g data rates.

The radio supports no encryption, WEP, LEAP or WPA (PEAP-MSCHAP, WPA/LEAP and WPA-PSK). *PEAP-GTC and EAP-TLS are not available in this release*. Contact your LXE representative for availability.

Summit Client Utility

Access: **Start | Programs | Summit | SCU** *or* **SCU Icon on Desktop**



Active Config: Default

Is Not Associated

SCU v1.01.10
Driver v1.01.10
WorldWide

Powered by DeviceScape
This product includes software
developed by the OpenSSL

Copyright © 2006 Summit Data Communications

Figure 4-1 Summit Client Utility

The **Main** tab provides information, admin login and active config (profile) selection.

Profile specific parameters are found on the **Config** tab. The parameters on this tab can be set to unique values for each profile.

The **Status** tab contains information on the current connection.

The **Diags** tab provides utilities to troubleshoot the radio.

Global parameters are found on the **Global Settings** tab. The values for these parameters apply to all profiles.

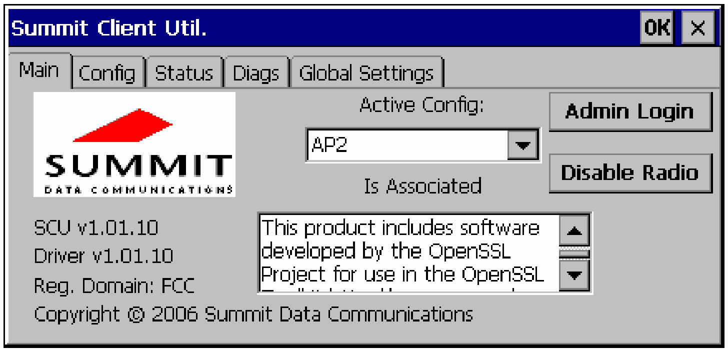
Wireless Zero Config Utility and the Summit Client

- The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled at this time and the MX3-RFID is not connected to a network.
- You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. See section titled "Wireless Zero Config Utility" at the end of this chapter.

Important: Perform a Warm Reset / Suspend and Resume function (after adding a new profile or changing parameters of an existing profile) to save the changed parameters in the registry.

Main Tab

Factory Default Settings	
Admin Login	SUMMIT
Radio	Enabled
Active Config	Default



Active Config: AP2

Is Associated

SCU v1.01.10

Driver v1.01.10

Reg. Domain: FCC

Copyright © 2006 Summit Data Communications

This product includes software developed by the OpenSSL Project for use in the OpenSSL

Figure 4-2 SCU – Main Tab

The Main tab displays information about the radio that includes the SCU (Summit Client Utility) version, radio driver version, regulatory domain, Summit copyright information, Active Config profile and status of the radio (e.g. Down, Associated, etc.).

The **Active Config** (profile) can be switched without logging in to Administrator mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. LXE recommends performing a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Administrator password has been entered and accepted.

The **Disable Radio** button is used to disable the radio card. Once disabled, the button label changes to Enable Radio.

The **Admin Login** button provides access to editing radio parameters. Config and Global Settings may only be edited after entering the Admin Login password. The password is case-sensitive. Once logged in, the button label changes to Admin Logout. To logout, either tap the Admin Logout button or exit the SCU without tapping the Admin Logout button.

Admin Login

Config and Global parameters may only be edited after entering the Admin Login password. The password is case-sensitive.

Once logged in, the button label changed to Admin Logout. The admin is automatically logged out when the SCU is exited.

The Admin can either tap the Admin Logout button, or a navigation button (X or OK), to logout.

The Admin remains logged in when the SCU is not closed and the mobile device is warmbooted.

To login to Admin mode, tap the Admin login button.

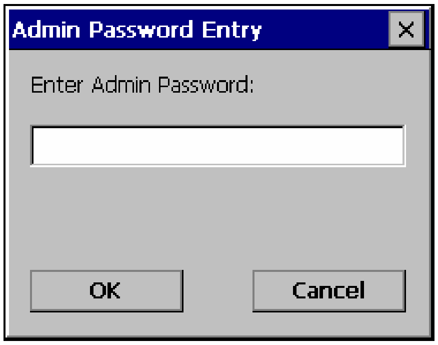


Figure 4-3 Admin Password Entry

Enter the Admin password and tap OK. If the password is incorrect, an error message is displayed. The default password is SUMMIT.

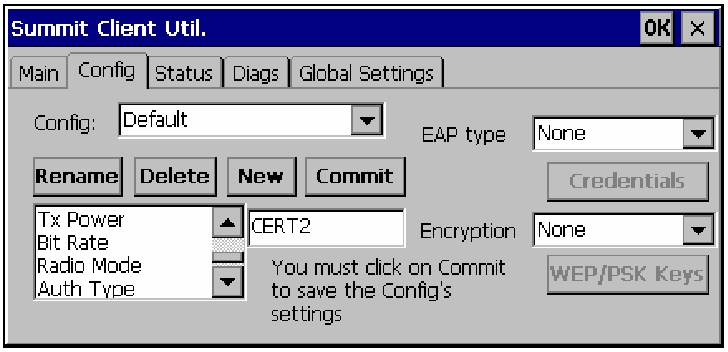
Note: The password is case sensitive!

The Admin password can be changed, by the administrator, using Global Settings.

Config Tab

*Note: Tap the **Commit** button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!*

Factory Default Settings	
Config Profile	Default
SSID	Blank
Client Name	Blank
Power Save	CAM
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	B+G rates
Auth Type	Open
EAP type	None
Encryption	None



Config: Default

EAP type: None

CERT2

Encryption: None

You must click on Commit to save the Config's settings

Figure 4-4 SCU – Config Tab

When logged in as an Admin (see "Admin Login"), use the Config tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, but cannot be changed.

Buttons

Button	Function
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.
New	Creates a new profile with the default settings (see "Config Parameters") and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.
WEP/PSK Keys	The **Encryption** type chosen determines if the WEP/PSK Keys button is active. Allows entry of WEP keys or pass phrase as required by the type of encryption.

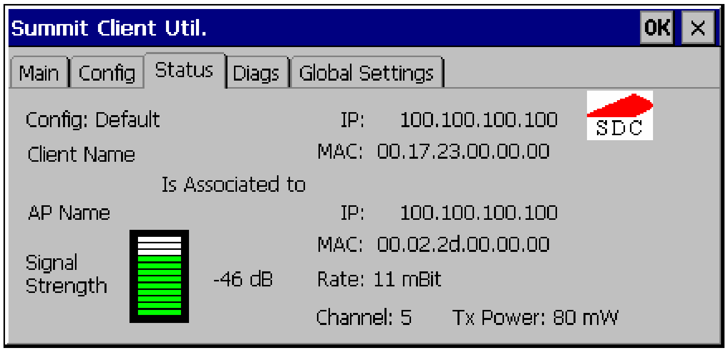
IMPORTANT – The settings for *Auth Type*, *EAP Type* and *Encryption* depend on the security type chosen. Please refer to “Wireless Security” later in this Summit Client Utility section to determine the proper settings for the security type implemented on the wireless LAN.

Config Parameters

Parameter	**Default**	**Explanation**
Config	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Config or Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the radio connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the radio and the device using the radio. The client name may be passed to networking radio devices, e.g. Access Points.
Power Save	CAM	Power save mode is Off. The radio is in Constantly Awake Mode (CAM).
Tx Power	Maximum	Maximum setting regulates Tx power to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 10mW or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the compact flash radio. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Radio Mode	B+G rates	Specify 802.11g and/or 802.11b when communicating with the Access Point. Options are: B rates only or B+G rates.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, or EAP-TLS. *Note: EAP Type chosen determines whether the **Credentials** button is active and also determines the available entries in the Credentials pop-up window.*

Parameter	Default	Explanation
Encryption	None	Type of encryption to be used to protect transmitted data. Options are: None, Manual WEP, Auto WEP, WPA PSK, WPA TKIP, WPA2 PSK, WPA2 TKIP, WPA2 AES, CCKM TKIP, or CCKM AES. *Note: The Encryption type chosen determines if the **WEP/PSK Keys** button is active and also determines the available entries in the WEP or PSK pop-up window.*

Status



Config: Default IP: 100.100.100.100
Client Name MAC: 00.17.23.00.00.00
Is Associated to
AP Name IP: 100.100.100.100
MAC: 00.02.2d.00.00.00
Signal Strength -46 dB Rate: 11 mBit
Channel: 5 Tx Power: 80 mW

Figure 4-5 SCU – Status Tab

This screen displays information on the current profile and radio connection. Information cannot be edited or changed on the Status panel. The panel displays:

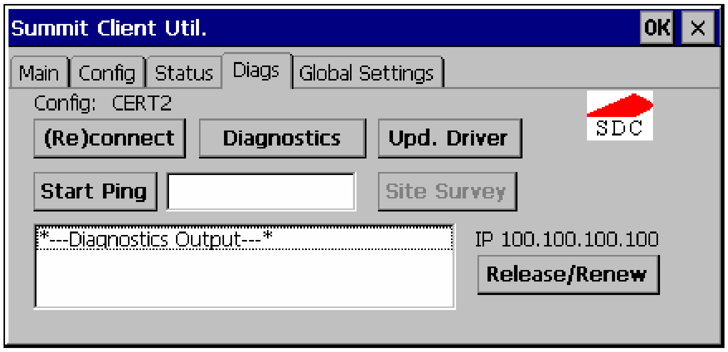
- The config profile being used
- The client name, IP address and MAC address
- The status of the radio connection (down, associated, etc.)
- The name, IP address and MAC address of the Access Point maintaining the connection to the network.
- Signal strength (changes with network activity).
- Channel currently being used for wireless traffic.
- Current transmit power in mW.
- Bit rate in Mbit.

Diags Tab

The Diags panel can be used for troubleshooting network traffic and radio connectivity issues for the IP address shown above the Release/Renew button. The Diags panel can also be used to update the radio driver on the MX3-RFID.

Administrator login is required for the (Re)connect button function.

Note: Diagnostics, Update Driver and Site Survey functions are not available in this release.



Config: CERT2

---Diagnostics Output---

IP 100.100.100.100

Figure 4-6 SCU – Diags Tab

Buttons

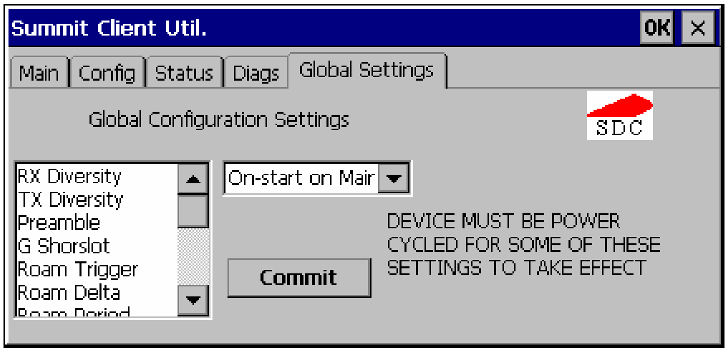
Button	Function
(Re)connect	Tap this button to apply, or reapply, the current config profile and attempt to associate or authenticate to the wireless LAN. Activity is logged in the Diagnostic Output text box on the lower part of the panel. Administrator login required for this function.
Release/Renew	Release the current IP address to obtain a new IP address. This option renews the IP address when applicable. Activity is logged in the Diagnostic Output text box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. The current IP address is displayed above the Release/Renew button.
Start Ping	Tap the text box and type an IP address to Ping. Tap the Start Ping button to start pinging the IP address. The button name changes to Stop Ping. Tap Stop Ping to end the pinging process. The pinging process ends when any other button on this panel is tapped or a different menu tab is selected. Ping results are displayed in the Diagnostic Output text box.
Diagnostics	Tapping this button begins an attempt to (re)connect to the wireless LAN. This option provides more data in the Diagnostics Output text box than the (Re)connect option. The data dump includes radio state, profile settings, global settings, and a list of access points by SSID broadcasting in the radio's immediate area. *Not available in this release.*
Update Driver	Tap this button to begin the process to update the radio driver via a dialog box and a power cycle. The radio driver file needs to be accessible to the user. *Not available in this release.*
Site Survey	*Not available in this release.*

Global Settings Tab

The parameters on the Global Settings panel can only be changed when an Administrator is logged in. No password is required to view the parameter settings.

*Note: Tap the **Commit** button to save changes. If the panel is closed before tapping the Commit button, changes are not saved!*

Factory Default Settings	
RX Diversity	On-Start on Main
TX Diversity	On
Preamble	Auto
G Shorslot	Auto
Roam Trigger	-65 dBm
Roam Delta	10 dBm
Roam Period	10 sec.
Frag Threshold	2346
RTS Threshold	2347
Ping Payload	32 bytes
Ping Timeout	5000
Ping Delay ms	1000
LED	Off
Hide Passwords	On
Admin Password	Blank
Certs Path	System



Global Configuration Settings

RX Diversity
TX Diversity
Preamble
G Shorslot
Roam Trigger
Roam Delta
Roam Period

On-start on Mair

DEVICE MUST BE POWER CYCLED FOR SOME OF THESE SETTINGS TO TAKE EFFECT

Figure 4-7 SCU – Global Settings Tab

Global Parameters

Note: Tap the ***Commit*** *button to save changes. If the panel is closed before tapping the Commit button, changes are not saved!*

Parameter	**Default**	**Function**
RX Diversity	On-start on Main	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only), Aux Only (use the auxiliary antenna only), On-start on Main (on startup, use the main antenna), or On-start on Aux (on startup, use the auxiliary antenna).
TX Diversity	On	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only), Aux only (use the auxiliary antenna only), or On (use diversity or both antennas).
Preamble	Auto	The type of radio header, or preamble, for packets. Options are: Auto, Short, or Long.
G Shortslot	Auto	802.1x short slot timing mode. Options are: Auto, On, or Off.
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the radio looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, or -75 dBm.
Roam Delta	10 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, or 35 dBm.
Roam Period	10 sec	The amount of time to be used to collect signal strength information from an Access Point before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, or 60 sec.
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. Options are: Any number between 256 bytes and 2346 bytes.

Parameter	Default	Function
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.
LED	Off	The LED on the radio card is not visible to the user when the radio card is installed in a sealed mobile device. Options are: On, Off.
Hide Password	On	If On, the Summit Config Utility masks passwords as they are typed and when they are viewed. Options are: On, Off.
Admin Password	SUMMIT	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry text box. The password is case sensitive. Options are: none.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device. LXE suggests ensuring the directory path currently exists before assigning the path in this parameter. See sections titled “Root Certificates” and “User Certificates” later in this chapter for instructions on obtaining CA and User Certificates. Options are: none.

Summit Wireless Security

Use the instructions in this section to complete the entries on the Config tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your System Administrator for complete information about your network and its wireless security requirements.

Note: It is important that all dates are correct on CE computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

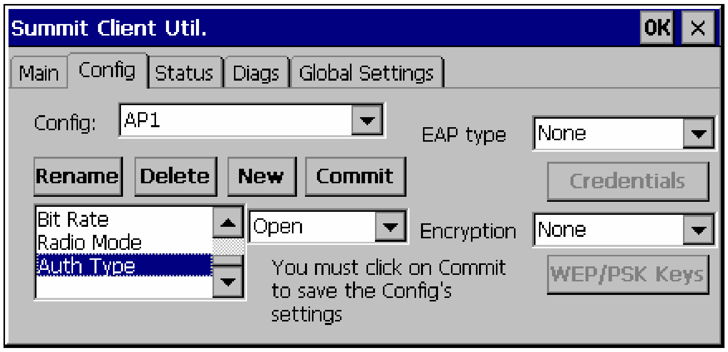
Default profile	LXE recommends editing the Default profile instead of creating new profiles. **Important**: Perform a soft reset (or Suspend/Resume) after changing parameters to save the changed parameters in the registry.
Switching profiles	Successfully connecting after switching from one profile to another may take up to 30 seconds from the moment the "Is not authenticated" message is displayed.
Adding/changing profiles	LXE recommends performing a Warmboot function (or Suspend/Resume) after tapping the Commit button.

No Security

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel**.** Enter the Administrator **password** and tap OK.

Tap the **Config** tab.



Config: AP1

EAP type: None

Open

Encryption: None

You must click on Commit to save the Config's settings

Figure 4-8 Summit Profile with No Security

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to None.

Tap the **Commit** button [2] to save the new profile configuration.

Perform a **warm reset** to connect using the new profile configuration.

[2] LXE recommends performing a soft reset or Suspend/Resume function each time the Commit button is tapped.

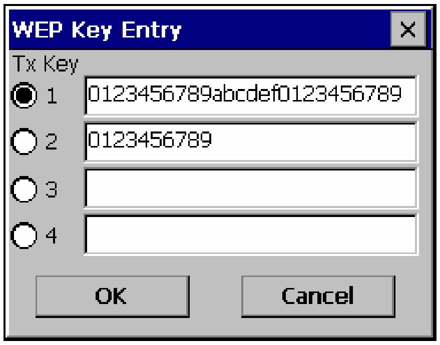
WEP Keys

Please see your System Administrator for complete information about your network WEP key requirements.

To connect using WEP, use the following minimum required profile options..

- Auth Type = Open
- EAP Type = None
- Encryption = Manual WEP

Tap the **WEP/PSK** Keys button. The WEP Key Entry text entry box appears.



WEP Key Entry

Tx Key

● 1 0123456789abcdef0123456789

○ 2 0123456789

○ 3

○ 4

Figure 4-9 Summit WEP Keys

Enter the **WEP key**. If there are more than one set of keys, tap the radio button in front of the Key to be used.

Valid values are 10 characters (for 40 bit encryption) or 26 characters (for 128 bit encryption) hexadecimal characters.

Tap **OK**. Tap the **Commit** button. Warm boot the mobile device.

LEAP w/o WPA Authentication

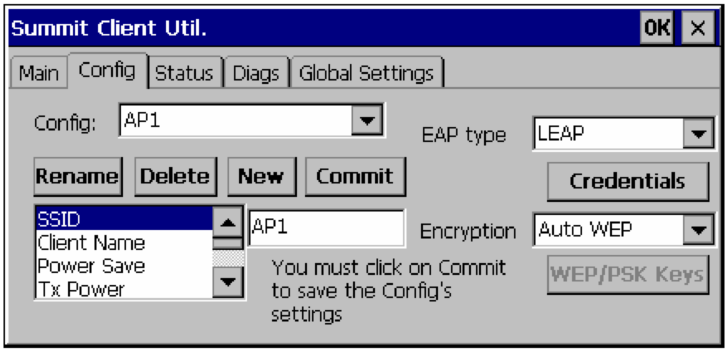
If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to “Open”.

If the AP is configured for network EAP only, set the Auth Type radio parameter to “LEAP”.

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel**.** Enter the Administrator **password** and tap OK.

Tap the **Config** tab.



Summit Client Util.

Config: AP1

EAP type: LEAP

SSID: AP1

Encryption: Auto WEP

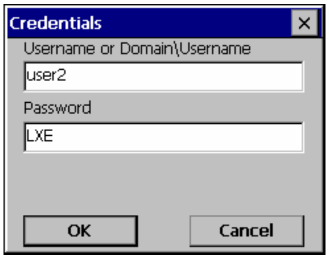
You must click on Commit to save the Config's settings

Figure 4-10 Summit Profile for LEAP w/o WPA

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open. Set **EAP Type** to LEAP.

Set **Encryption** to Auto WEP. Tap the **Credentials** button.



Credentials

Username or Domain\Username: user2

Password: LXE

Figure 4-11 Summit LEAP Credentials

Enter the **Username** or Domain \Username in the Credentials popup text entry box.

Enter the **Password**. Tap **OK**. Tap the **Commit** button to save the new profile configuration.

Perform a **warm reset** to connect using the new profile configuration.

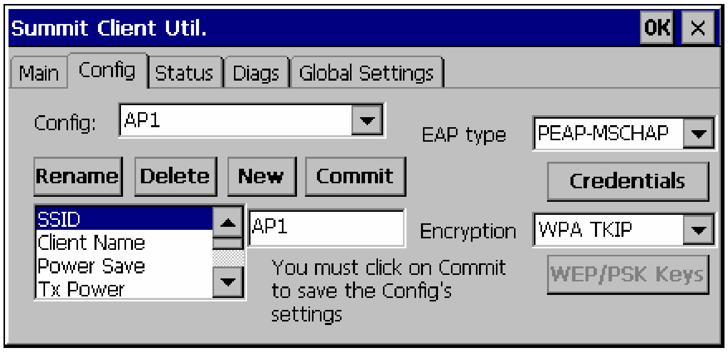
Please see “WPA/LEAP Authentication” later in this section to configure the radio for WPA LEAP.

PEAP/MSCHAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel. Enter the Administrator **password** and tap OK.

Tap the **Config** tab.



Config: AP1

EAP type PEAP-MSCHAP

SSID AP1

Encryption WPA TKIP

You must click on Commit to save the Config's settings

Figure 4-12 Summit Profile for PEAP/MSCHAP

Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to PEAP-MSCHAP.

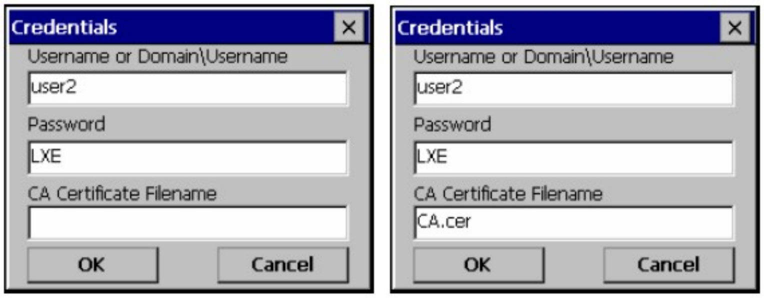
Set **Encryption** to Auto WEP (without WPA). To configure PEAP-MSCHAP for WPA set Encryption to WPA TKIP.

Tap the **Credentials** button.

Enter the **Username** or Domain\Username in the Credentials popup text entry box.

Enter the **Password**.

Leave the CA Certificate Filename blank for now.



Credentials

Username or Domain\Username

user2

Password

LXE

CA Certificate Filename

Credentials

Username or Domain\Username

user2

Password

LXE

CA Certificate Filename

CA.cer

Figure 4-13 Summit PEAP/MSCHAP Credentials

Once successfully authenticated, copy the CA certificate into the \System directory of the device. Once the file is in the \System directory, enter the file name in the CA Certificate Filename text box.

Tap **OK** then tap **Commit**. Perform a warm reset function.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

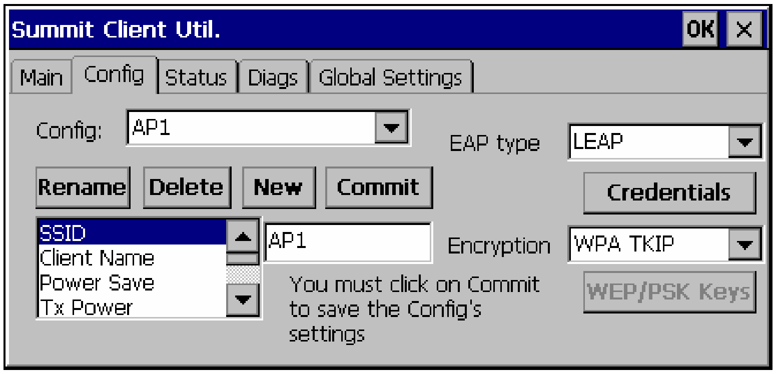
Note: The date must be properly set on the mobile device to authenticate a certificate.

WPA/LEAP Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel**.** Enter the Administrator **password** and tap OK.

Tap the **Config** tab.



Config: AP1

EAP type LEAP

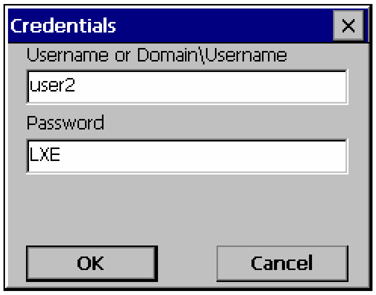
SSID AP1

Encryption WPA TKIP

You must click on Commit to save the Config's settings

Figure 4-14 Summit Profile with LEAP for WPA TKIP

Tap the **Credentials** button.



Username or Domain\Username: user2

Password: LXE

Figure 4-15 Summit WPA/LEAP Credentials

Enter the **Username** or Domain \Username in the Credentials popup text entry box.

Enter the **Password**. Tap **OK**.

Tap the **Commit** button to save the new profile configuration.

Perform a **warm reset** to connect using the new profile configuration.

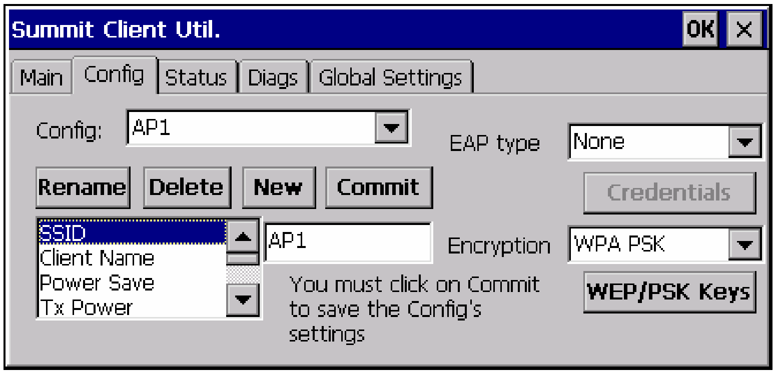
Please see "LEAP w/o WPA" earlier in this section to configure the radio for LEAP without WPA.

WPA PSK Authentication

Start the Summit Utility by tapping the Summit Client icon.

Tap the **Admin Login** button on the Main panel**.** Enter the Administrator **password** and tap OK.

Tap the **Config** tab.



Config: AP1

EAP type: None

SSID: AP1

Encryption: WPA PSK

You must click on Commit to save the Config's settings

Figure 4-16 Summit Profile with WPA/PSK Encryption

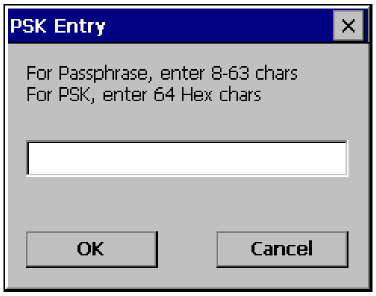
Enter the **SSID** of the Access Point assigned to this profile.

Set **Auth Type** to Open.

Set **EAP Type** to None.

Set **Encryption** to WPA PSK.

Tap the **WEP/PSK Keys** button.



For Passphrase, enter 8-63 chars
For PSK, enter 64 Hex chars

Figure 4-17 Summit PSK Entry

Enter the Passphrase in the **PSK Entry** popup text entry box. This value can be a 64 hex character or an 8-63 byte ASCII value. Tap **OK**

Tap the **Commit** button to save the new profile configuration.

Perform a **warm reset** to connect using the new profile configuration.

Tap the **Main** tab. The screen shows the "WPA PSK" Active Config is **Associated** after the radio connects to the network.

Cisco Client Configuration

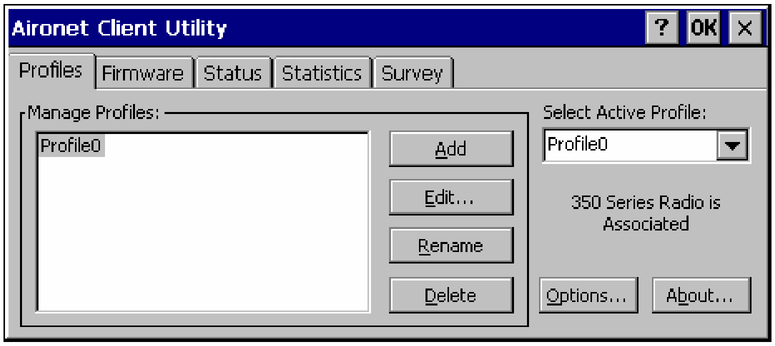
Prerequisites

- Network SSID or ESSID number of the Access Point
- WEP or LEAP Authentication Protocol Keys

Aironet Client Utility (ACU)

Access: Start | Aironet Client Utility *or* ACU Icon on Desktop

Note: When making changes to profile parameters, the mobile device should be warmbooted afterwards.



Manage Profiles:
Profile0

Select Active Profile: Profile0

350 Series Radio is Associated

Figure 4-18 Cisco Aironet Client Utility

Note: To configure WPA, please see "Cisco Configuration", later in this chapter.

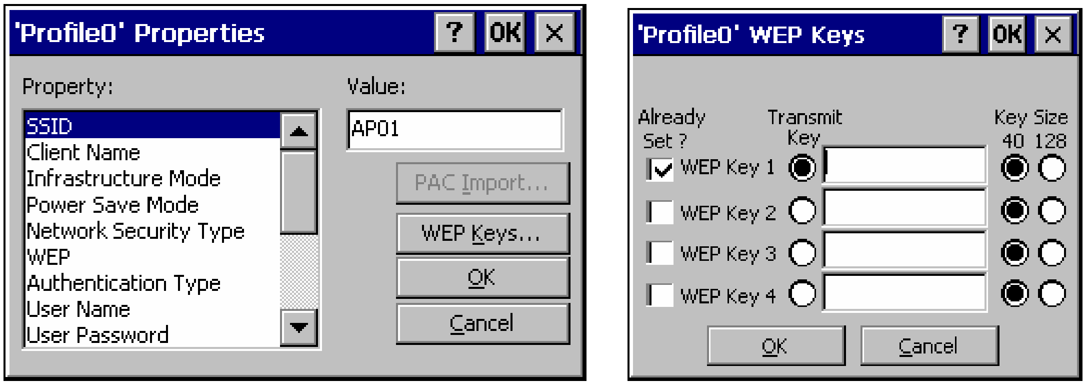
Profiles Tab	See the following "Profiles Tab" section for default profile parameter settings.
Firmware Tab	Displays the current firmware version and allows you to load new firmware. Tap the Browse button to locate the new firmware file.
Status Tab	Immediately runs status on : signal strength and signal quality.
Statistics Tab	Select the Receive Stats or Transmit Stats. The data is displayed on the screen.
Survey Tab	Immediately runs signal strength and quality and link speed. An option is available to Setup parameters for Active Mode reporting.

Profile Parameters

Use this option to manage profiles and review firmware information, status, statistics and wireless radio survey data.

Profile Parameter	Default
SSID	Blank
Client Name	Blank
Infrastructure Mode	Yes
Power Save Mode	Fast PSP
Network Security Type	None
WEP	No WEP
Authentication Types	Open
LEAP	Disabled
Mixed Mode	Disabled
World Mode	Disabled
Data Rates	Auto
Transmit Power	MAX
Offline Channel Scan	Enabled

Select an active profile to manage.



'Profile0' Properties

Property:
- SSID
- Client Name
- Infrastructure Mode
- Power Save Mode
- Network Security Type
- WEP
- Authentication Type
- User Name
- User Password

Value: AP01

'Profile0' WEP Keys

Already Set ?		Transmit Key		Key Size 40	128
☑	WEP Key 1	●		●	○
☐	WEP Key 2	○		●	○
☐	WEP Key 3	○		●	○
☐	WEP Key 4	○		●	○

Figure 4-19 Cisco Profile Properties Screen

Tap the **WEP Keys** button to enter WEP information. If a key is already entered, the "Already set?" checkbox is checked. The previously entered key value is not displayed for security.

Cisco Wireless Security

Wi-Fi Protected Access (WPA) is only available on mobile device's equipped with the updated radio driver (**release 2.60 or later**).

WPA requires software **revision 1ED** or greater. To identify the software revision, please tap the "About" icon in the Control Panel.

📖	Please refer to the "LXE Security Primer" to prepare the Authentication Server and Access Point for Cisco wireless communication.

Date/Time	It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

System Requirements

To support Wi-Fi Protected Access (WPA), the mobile device must be equipped as follows:

- Cisco 350 radio card with driver release 2.60 (or later).

The radio supports WPA and all authentications. The Microsoft supplicant and Cisco supplicants are used separately or together to provide support for the different authentications.

Most of the configuration is done with the Microsoft Wireless Configuration tool.

WPA/LEAP requires the Cisco supplicant and Cisco ACU configuration tool.

Installing Radio drivers

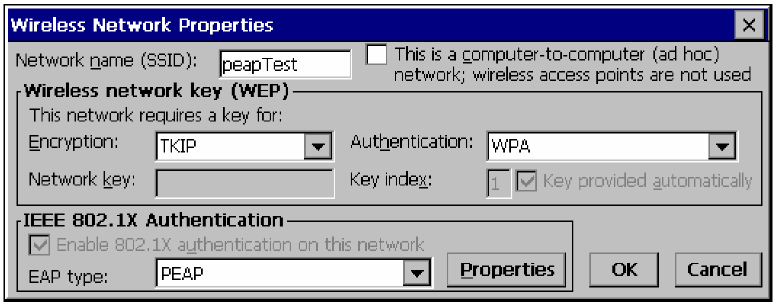
Which version of the Cisco driver should be installed depends on which authentication protocol is to be configured.

- Cisco PEAP should not be installed if using PEAP/MSCHAP.
- Cisco PEAP must be installed if using PEAP/GTC.
- For all other authentications (LEAP, EAP-TLS, WPA-PSK) it does not matter if Cisco PEAP is installed or not.

To determine if Cisco PEAP is installed or to change the installation, refer to the instructions in the following sections.

Checking for the Cisco PEAP Supplicant

With a radio installed, open the Wireless network properties as described in “Cisco Configuration”, later in this section. With the Authentication tab selected check the text in the EAP type drop down box. Refer to the following figures to determine if Cisco PEAP is installed.



Wireless Network Properties

Network name (SSID): peapTest

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

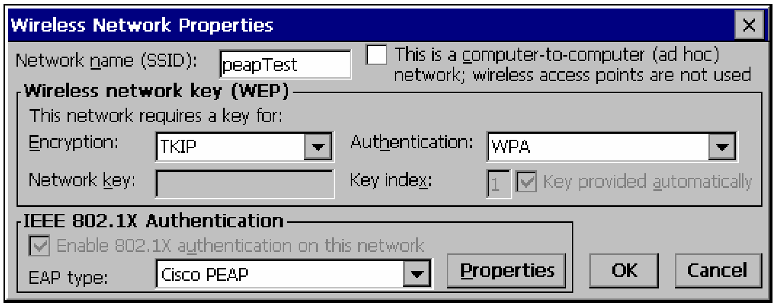
☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: PEAP

Figure 4-20 No Cisco PEAP



Wireless Network Properties

Network name (SSID): peapTest

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: Cisco PEAP

Figure 4-21 Cisco PEAP Installed

If the Cisco installation is correct, continue with the configuration. If it is not correct, follow the procedures below.

Note: Instructions are also included in the README file located in the \SYSTEM folder.

There are two Cisco CAB files in the \SYSTEM folder. The default files are:

CISCO.CAB **CISCOPEAP.CAB**

The default CISCO.CAB file provides for all authentications except Cisco PEAP. When the default CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the figure labeled “No Cisco PEAP”, above.

If Cisco PEAP is desired:

1. Rename the CISCO.CAB file to CISCOMSCHAP.CAB.
2. Rename the CISCOPEAP.CAB file to CISCO.CAB.
3. Coldboot the mobile device to install the new driver with the registry.

The renamed CISCO.CAB file provides for Cisco PEAP and PEAP/GTC authentications. When the renamed CISCO.CAB file is loaded, the Wireless Network Properties screen looks like the previous figure labeled “Cisco PEAP Installed”.

If it becomes necessary to switch to a different authentication than Cisco PEAP or PEAP/GTC,

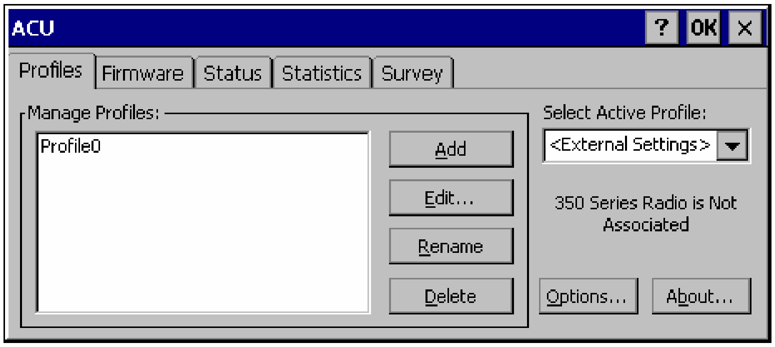
1. Rename the CISCO.CAB file to CISCOPEAP.CAB.
2. Rename the CISCOMSCHAP.CAB file to CISCO.CAB
3. Coldboot the mobile device to install the new driver with the registry.

Cisco WPA Configuration

Use the following instructions for all authentication protocols to configure the Microsoft Wireless Network configuration utility unless WPA/LEAP is used.

WPA/LEAP is configured with the Cisco ACU (see Section titled "WPA/LEAP Authentication Configuration").

Tap the **ACU icon** on the desktop.



Manage Profiles: Profile0

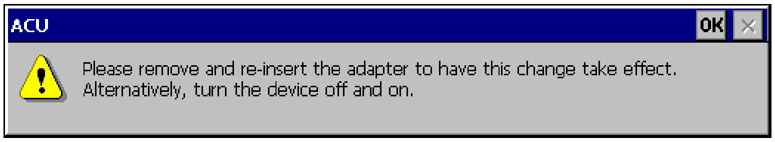
Select Active Profile: <External Settings>

350 Series Radio is Not Associated

Figure 4-22 Cisco ACU Profile Selection

From the **Select Active Profile** pull down list, select <External Settings>.

Tap **OK** and warmboot.



Please remove and re-insert the adapter to have this change take effect. Alternatively, turn the device off and on.

Figure 4-23 Cisco ACU Reboot Message

After booting up, the Microsoft Zero Config tool should start. If it does not, start configuring the wireless connection by tapping the icon on the task bar shown in below.

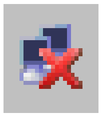
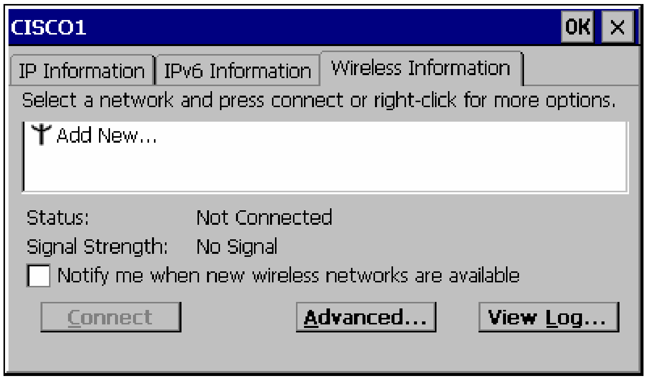


Figure 4-24 Microsoft Wireless Connection Icon

The Wireless Network Connection screen appears.



Select a network and press connect or right-click for more options.

Status: Not Connected

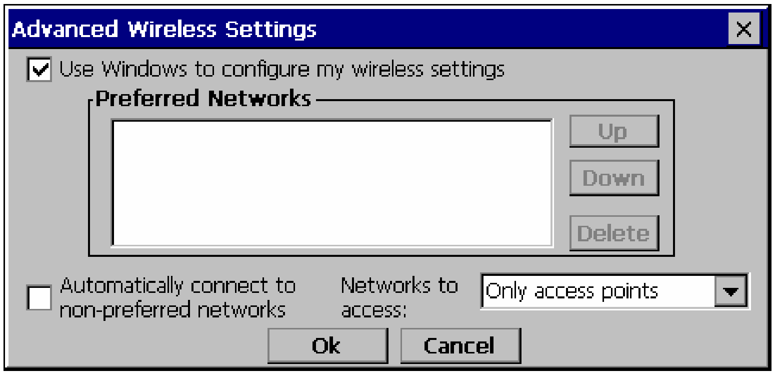
Signal Strength: No Signal

☐ Notify me when new wireless networks are available

Figure 4-25 Wireless Information Screen

Make sure the “Notify me when new wireless networks are available” box is *not* checked..

Tap the **Advanced**… button.



☑ Use Windows to configure my wireless settings

☐ Automatically connect to non-preferred networks

Networks to access: Only access points

Figure 4-26 Advanced Wireless Settings

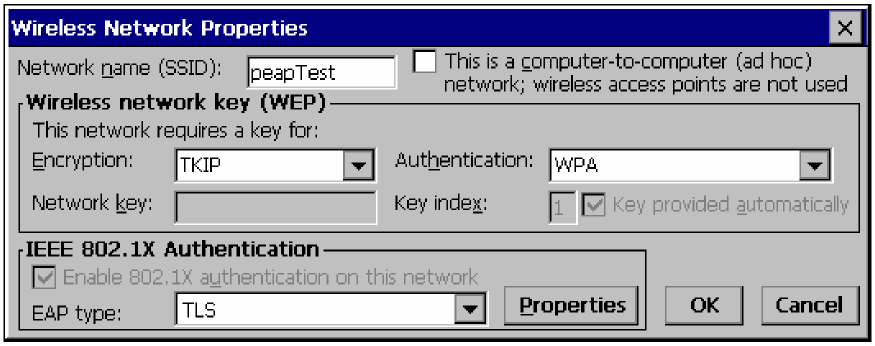
Make sure the “Use Windows to configure my wireless settings” box is checked.

Set the “Networks to access” drop down box to “Only access points”.

Tap the **OK** button on the Advanced Wireless Settings screen and the Wireless Information Screen is displayed.

On the Wireless Information screen tap the **Add New** … line.

The Wireless Network Properties screen is displayed.



Wireless Network Properties

Network name (SSID): peapTest

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: TLS

Figure 4-27 Wireless Network Properties

Enter the Network name (**SSID**) into the text field.

For PEAP/MSCHAP and EAP/TLS, set **Encryption** to TKIP and **Authentication** to WPA.

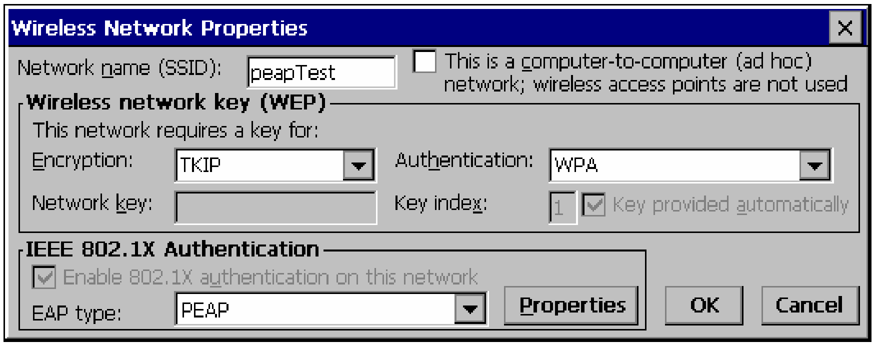
For WPA/PSK see “WPA/PSK Authentication Configuration”.

To configure the IEEE 802.1X Authentication box see the following sections for configuration of each authentication protocol.

PEAP/MS-CHAP Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/MS-CHAP protocol. The Cisco CAB file without Cisco PEAP must be used with PEAP/MS-CHAP. See “Installing Radio Drivers”, earlier in this chapter, for more information.

Configuring the PEAP/MS-CHAP Supplicant



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

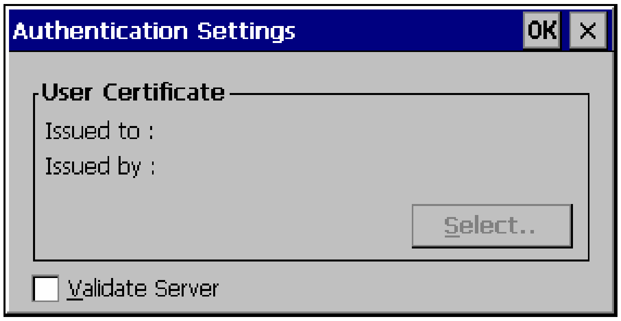
EAP type: PEAP

Figure 4-28 PEAP/MSCHAP Wireless Network Properties

With the radio parameters configured set the **EAP type** to PEAP as shown above.

If the EAP type box text is not exactly as shown see “Installing Radio Drivers” earlier in this chapter, to change the radio CAB file.

Tap the **Properties** button.



Authentication Settings

User Certificate

Issued to :

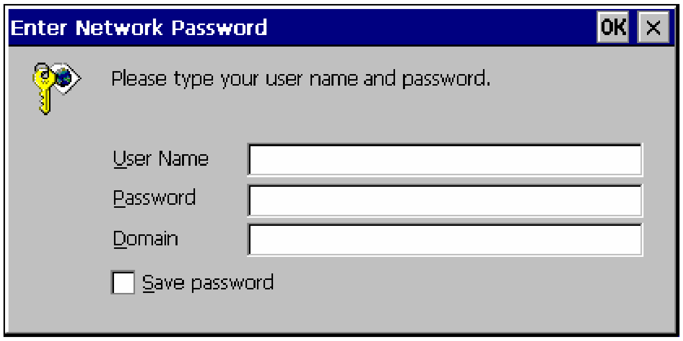
Issued by :

□ Validate Server

Figure 4-29 Authentication Settings

When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, come back to this screen and validate the server certificate.

The login screen appears for logging into the wireless network.



Enter Network Password

Please type your user name and password.

User Name

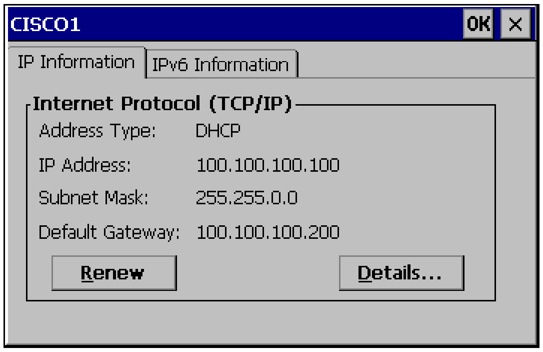
Password

Domain

□ Save password

Figure 4-30 Wireless Network Login

Once authenticated, tap the **IP Information** tab.



CISCO1

IP Information | IPv6 Information

Internet Protocol (TCP/IP)

Address Type:	DHCP
IP Address:	100.100.100.100
Subnet Mask:	255.255.0.0
Default Gateway:	100.100.100.200

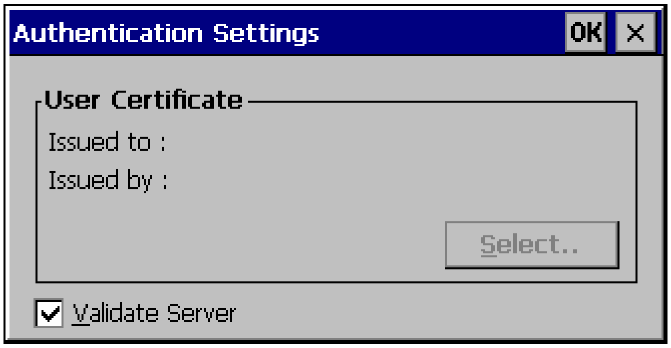
Figure 4-31 IP Information Tab

If the network is set to use DHCP, the mobile device displays the IP address assigned by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see “Root Certificates”, later in this chapter.



Authentication Settings

User Certificate

Issued to :

Issued by :

☑ Validate Server

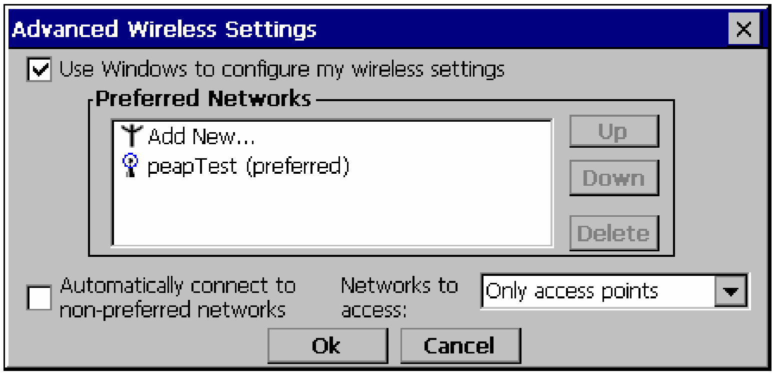
Figure 4-32 Authentication Settings, Validate Server

Navigate to the Wireless Network Properties configuration screen.

Tap the **Properties** button.

Check “Validate server” .

Tap **OK** to dismiss the configuration boxes.



☑ Use Windows to configure my wireless settings

□ Automatically connect to non-preferred networks

Networks to access: Only access points

Figure 4-33 Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the <SSID>, as shown in the figure above.

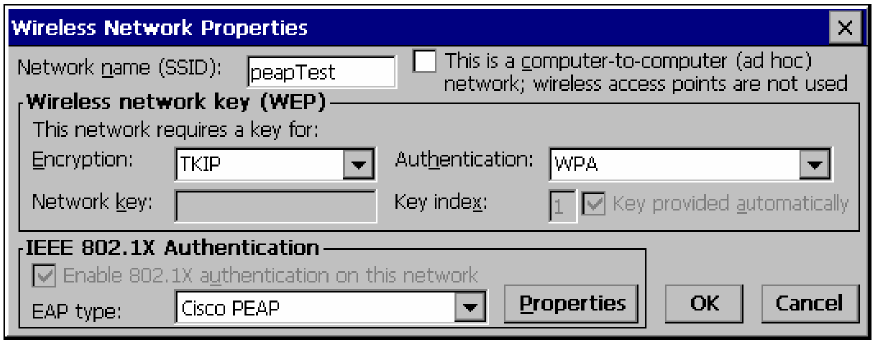
Tap the IP Information tab and make sure there is a valid IP address as shown in the figure labeled “IP Information Tab”, earlier in this chapter.

PEAP/GTC Authentication Configuration

The Microsoft supplicant authenticates a user with the PEAP/GTC protocol.

Configuring the PEAP/GTC Supplicant

With the radio parameters configured set the EAP type to Cisco PEAP as shown below.



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1

☑ Key provided automatically

IEEE 802.1X Authentication

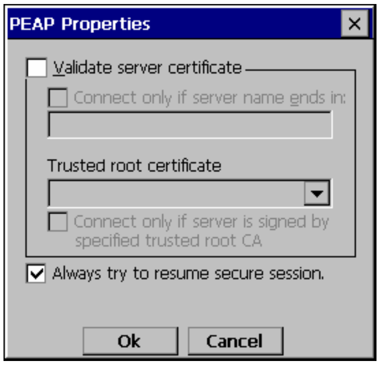
☑ Enable 802.1X authentication on this network

EAP type: Cisco PEAP

Figure 4-34 PEAP/GTC Wireless Network Properties

If the EAP type box text is not exactly as shown see “Installing Radio Drivers”, earlier in this chapter, to change the radio cab file.

Click the **Properties** button.



PEAP Properties

□ Validate server certificate

□ Connect only if server name ends in:

Trusted root certificate

□ Connect only if server is signed by specified trusted root CA

☑ Always try to resume secure session.

Figure 4-35 PEAP Properties

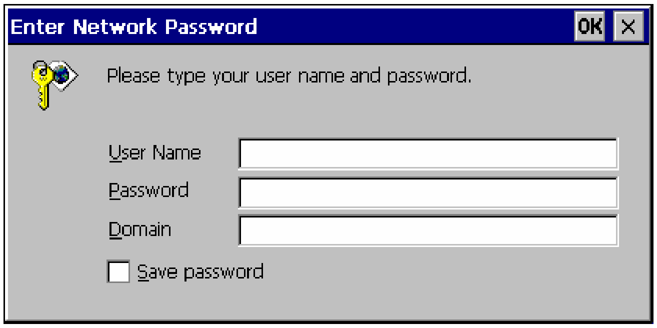
When first configuring and authenticating, do not validate the server certificate. This allows the user authentication to be tested. When user authentication is successful, return to this screen and validate the server certificate as shown later in this section.

Check the **Always try to resume secure session** box.

Note: This box must be checked for the LXE device to roam from one AP to another AP.

Tap the **OK** button.

The login screen appears for logging into the wireless network.

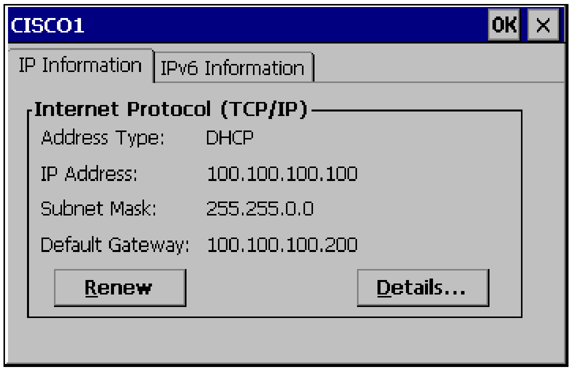


Please type your user name and password.

Figure 4-36 Login Screen

Enter valid user credentials.

Once authenticated tap the **IP Information** tab



Address Type: DHCP
IP Address: 100.100.100.100
Subnet Mask: 255.255.0.0
Default Gateway: 100.100.100.200

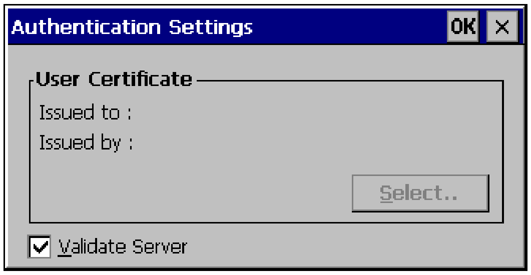
Figure 4-37 IP Information Tab

The .NET device displays the IP address given by the DHCP server.

Now go back and authenticate the server.

Server Authentication

To validate the server certificate install the root CA certificate. For instructions for installing, see “Root Certificates”, earlier in this chapter.



User Certificate

Issued to :

Issued by :

☑ Validate Server

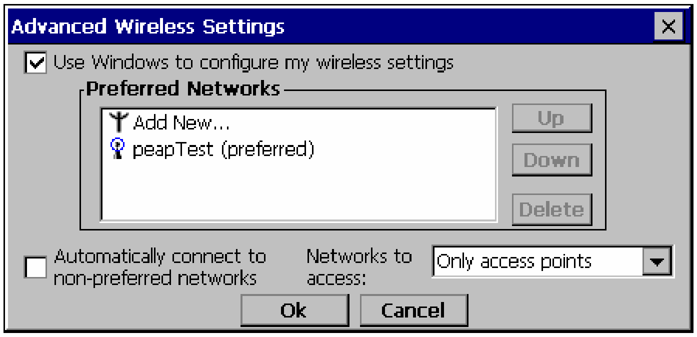
Figure 4-38 Authentication Settings, Validate Server

Navigate to the **Wireless Network Properties** configuration screen.

Tap the **Properties** button.

Check **Validate server** .

Tap **OK** to dismiss the configuration boxes.



☑ Use Windows to configure my wireless settings

Preferred Networks

Add New...

peapTest (preferred)

□ Automatically connect to non-preferred networks

Networks to access: Only access points

Figure 4-39 Advanced Wireless Settings, Authenticated SSID

Once the authentication completes, the status changes to show the mobile device has authenticated to the <SSID>, as shown in the figure above.

Tap the IP Information tab and make sure there is a valid IP address as shown in the figure labeled “IP Information Tab”, earlier in this chapter.

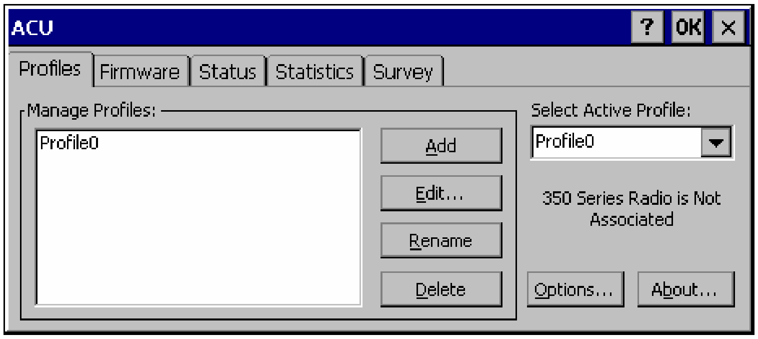
WPA/LEAP

LEAP is a Cisco proprietary authentication protocol and is not supported by the Microsoft supplicant. To configure the mobile device for WPA/LEAP, use the Cisco ACU installed during normal installation of the Cisco client driver.

Cisco ACU

Start the Cisco ACU by tapping the icon on the desktop or navigate to **Start | Programs | Cisco | ACU**.

Tap the Profile tab.



Manage Profiles: Profile0

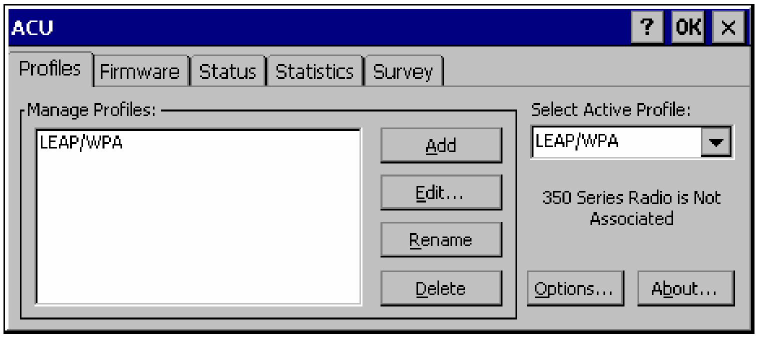
Select Active Profile: Profile0

350 Series Radio is Not Associated

Figure 4-40 WPA/LEAP using ACU Profile Tab

Tap the **Rename** button.

Name the profile.



Manage Profiles: LEAP/WPA

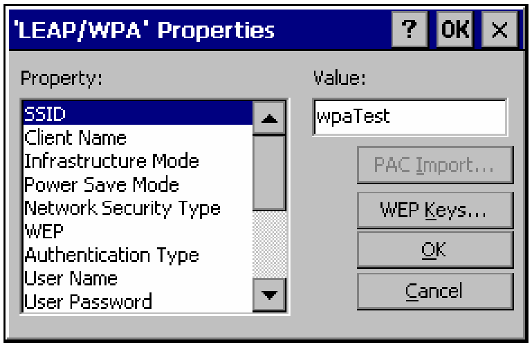
Select Active Profile: LEAP/WPA

350 Series Radio is Not Associated

Figure 4-41 Renaming Profile

Tap the **Edit** . . . button.

The profile properties screen is displayed.



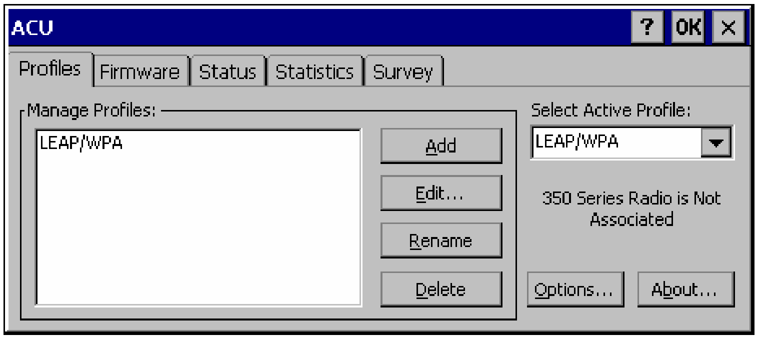
Value: wpaTest

Figure 4-42 Profile Properties Screen

Enter the **SSID** and **Client Name** in the correct fields.

Set the **Network Security Type** to LEAP(WPA).

Tap the **OK** button.



Select Active Profile: LEAP/WPA

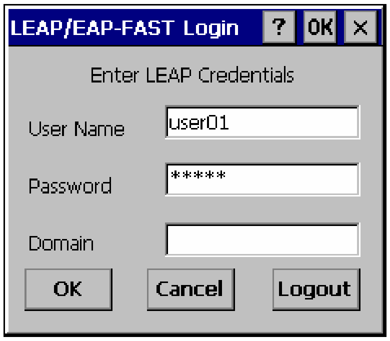
350 Series Radio is Not Associated

Figure 4-43 Select Profile

Use the drop down box to choose the profile just configured.

Tap **OK**.

The mobile device associates and displays the sign on screen.



Enter LEAP Credentials

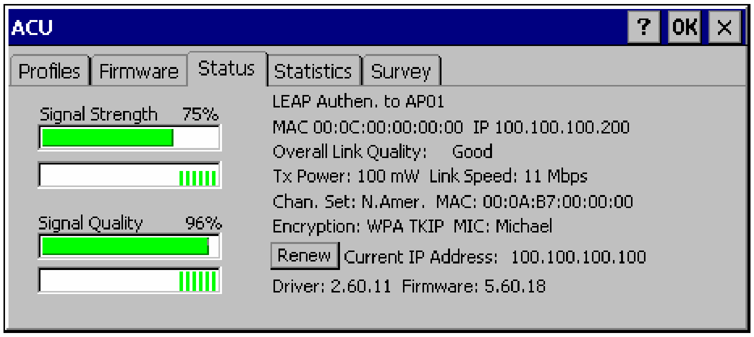
User Name user01

Password *****

Domain

Figure 4-44 Login Screen

Tap the **Status** tab to display status.



Signal Strength 75%

Signal Quality 96%

LEAP Authen. to AP01
MAC 00:0C:00:00:00:00 IP 100.100.100.200
Overall Link Quality: Good
Tx Power: 100 mW Link Speed: 11 Mbps
Chan. Set: N.Amer. MAC: 00:0A:B7:00:00:00
Encryption: WPA TKIP MIC: Michael
Current IP Address: 100.100.100.100
Driver: 2.60.11 Firmware: 5.60.18

Figure 4-45 ACU Status Tab

EAP-TLS Authentication Configuration

To authenticate using the EAP-TLS protocol you need a user certificate file and a private key file. Once you have the user certificate files run the certificate installer from the Microsoft control panel. For EAP-TLS it does not matter which Cisco cab file is installed.

Note: It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

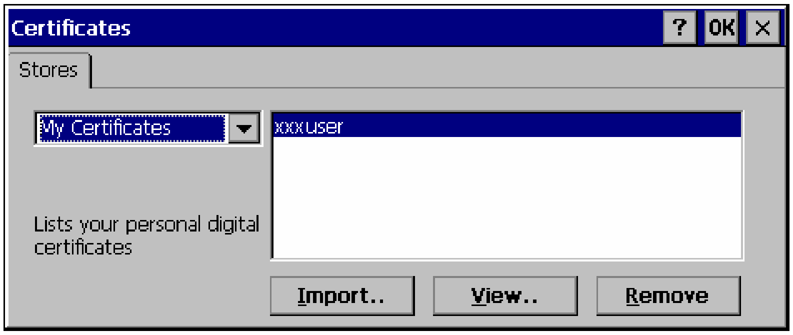
User Certificate

To check if a user certificate is installed navigate to **Start | Control Panel | Certificates**.

Certificates

Set the drop down box to "My Certificates" as shown below.

The correct user certificate should be shown in the right pane.


Certificates

Stores

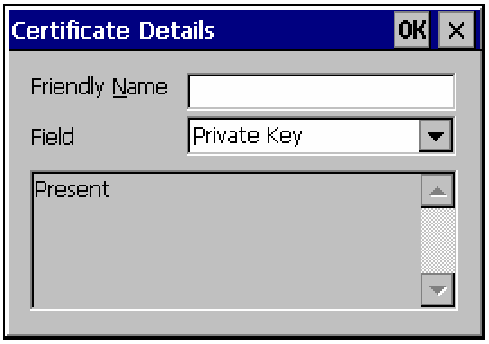
My Certificates

xxxuser

Lists your personal digital certificates

Figure 4-46 Certificate Stores

Tap the View . . . button.


Certificate Details

Friendly Name

Field: Private Key

Present

Figure 4-47 View Certificate Details

Set the **Field** to Private Key.

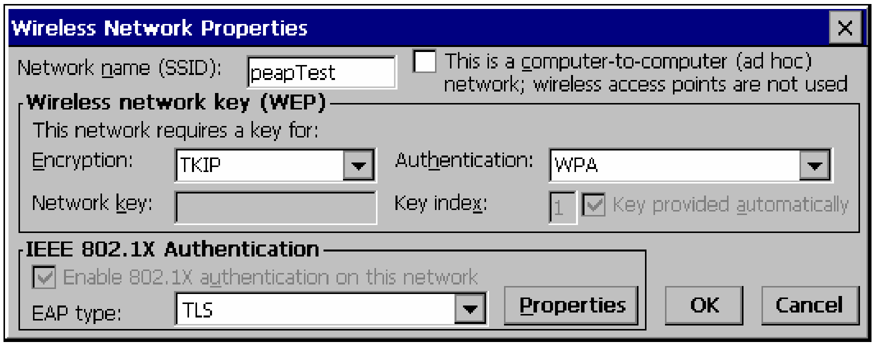
Make sure the private key is Present.

If it is not present, install the private key file.

If there is no user certificate refer to “User Certificates”, earlier in this chapter, to acquire a user certificate and private key file.

Setting EAP/TLS Parameters

With the radio parameters configured set the EAP type to TLS as shown.



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA

Network key:

Key index: 1 ☑ Key provided automatically

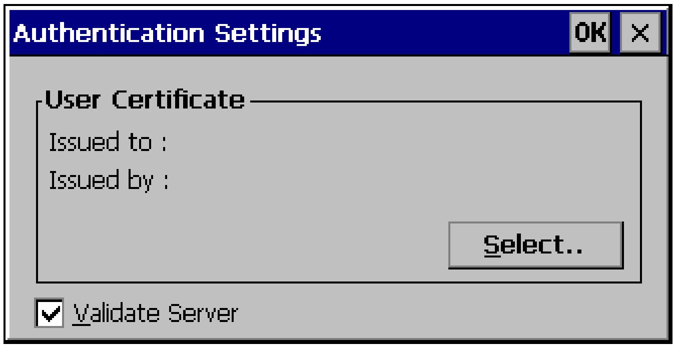
IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: TLS

Figure 4-48 EAP/TLS Configuration

Tap the **Properties** button.



Authentication Settings

User Certificate

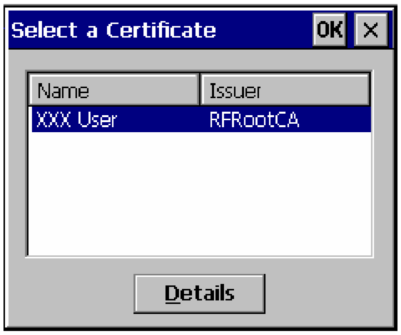
Issued to :

Issued by :

☑ Validate Server

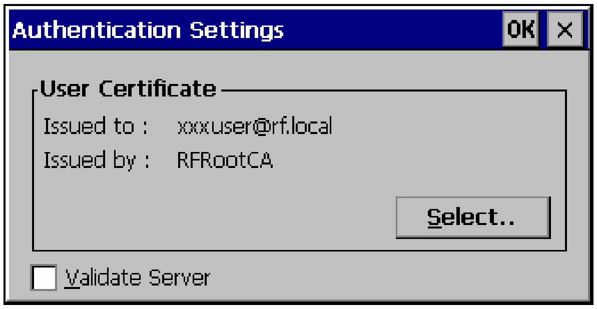
Figure 4-49 Authentication Settings

Tap the **Select** button to choose the user certificate.



Name	Issuer
XXX User	RFRootCA

Figure 4-50 Select Certificate



Issued to : xxxuser@rf.local

Issued by : RFRootCA

□ Validate Server

Figure 4-51 Authentication Settings, Certificate Details

Do *not* check the Validate server certificate box. This allows the user to be authenticated as the first step.

When the user certificate successfully authenticates, come back to this screen and validate the server certificate as described in the next section.

Tap the OK button to dismiss the configuration screens.

When the radio re-connects the user is authenticated with the user certificate.

If the user does not authenticate, recheck the user certificate and the date on the computer.

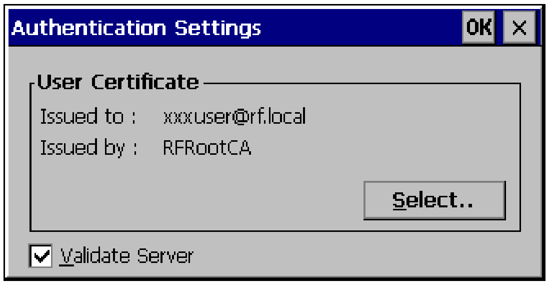
Validating the Server Certificate

Before validating the server certificate, make sure the Root CA certificate is installed on the mobile device.

Navigate to the Wireless Network Properties configuration screen.

Tap the **Properties** button.

Check the **Validate server** box as shown below.



Authentication Settings

User Certificate

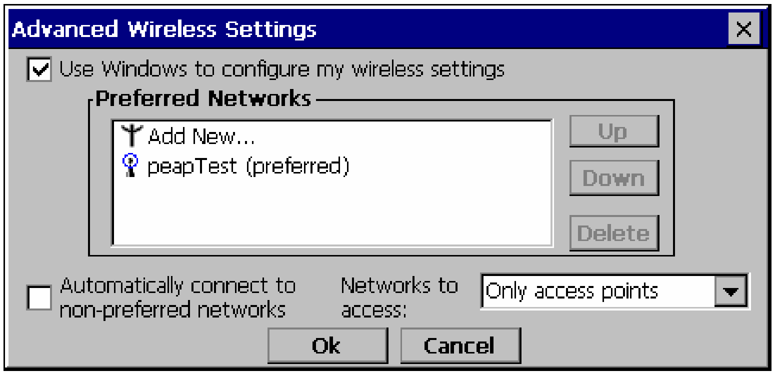
Issued to : xxxuser@rf.local

Issued by : RFRootCA

☑ Validate Server

Figure 4-52 Validate Server

Tap OK to dismiss the configuration boxes.



Advanced Wireless Settings

☑ Use Windows to configure my wireless settings

Preferred Networks

- Add New...
- peapTest (preferred)

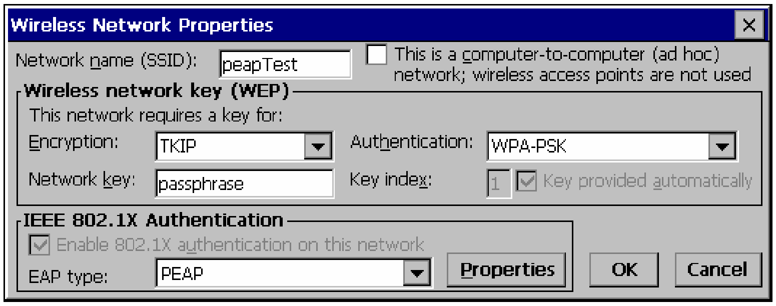
☐ Automatically connect to non-preferred networks

Networks to access: Only access points

Figure 4-53 SSID Authenticated

Once the authentication completes the status changes to show the mobile device has authenticated to <SSID> as shown above.

WPA PSK Configuration



Wireless Network Properties

Network name (SSID): peapTest

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network key (WEP)

This network requires a key for:

Encryption: TKIP

Authentication: WPA-PSK

Network key: passphrase

Key index: 1 ☑ Key provided automatically

IEEE 802.1X Authentication

☑ Enable 802.1X authentication on this network

EAP type: PEAP

Figure 4-54 WPA PSK Configuration

Configure the Wireless Network Settings as described in “Wireless Security”, earlier in this chapter.

Change the Network Authentication to **WPA-PSK**.

Enter an ASCII **network key** in the text field. Hex keys do not work in the Microsoft Zero Config utility at this time.

There is no server authentication when using WPA-PSK.

Tap the OK button to complete the configuration.

Certificates

Date/Time	It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Note: A pre-existing ActiveSync relationship between the desktop/laptop computer and the mobile device is required. LXE recommends installing a fully charged main battery before initiating a certificate file download to the mobile device.

Root Certificates

Generating a Root CA Certificate

Please refer to the “LXE Security Primer” for more information on obtaining and installing root certificates.

The easiest way to get the root CA certificate is to use a browser on a desktop PC to navigate to the CA (Certificate Authority). To request the root CA certificate, open a browser to

http://<CA IP address>/certsrv

Sign into the CA with any valid username and password.

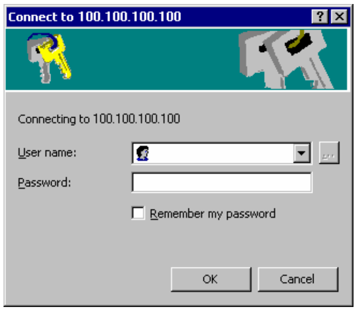
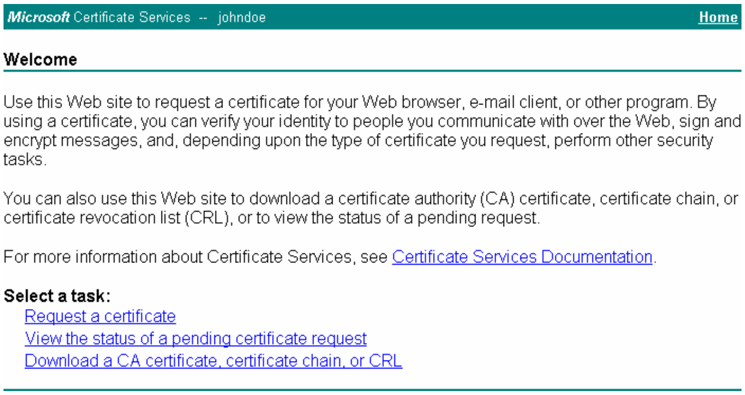


Figure 4-55 Logon to Certificate Authority



Microsoft Certificate Services -- johndoe **Home**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

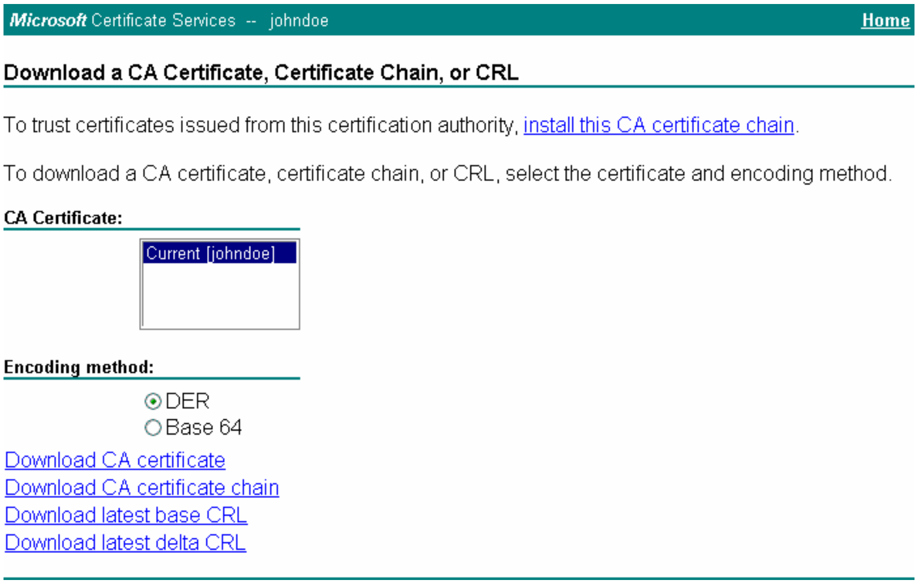
Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Figure 4-56 Certificate Services Welcome Screen

Click the **Download a CA certificate, certificate chain or CRL** task link.

Make sure the correct root **CA certificate** is selected in the list box.



Microsoft Certificate Services -- johndoe

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA Certificate: Current [johndoe]

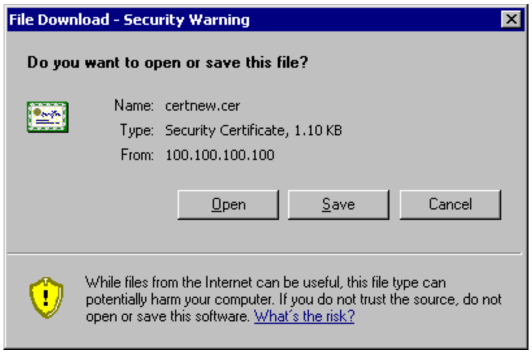
Encoding method:

● DER
○ Base 64

Figure 4-57 Download CA Certificate Screen

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.



File Download - Security Warning

Do you want to open or save this file?

Name: certnew.cer
Type: Security Certificate, 1.10 KB
From: 100.100.100.100

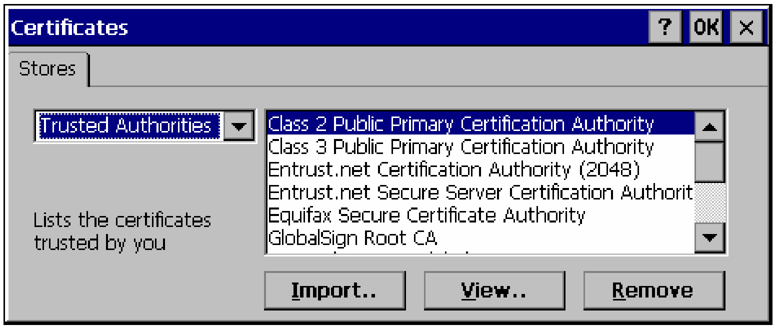
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Figure 4-58 Download CA Certificate Screen

Click the **Save** button and save the certificate to the desktop PC. Keep track of the name and location of the certificate as the certificate file name and file location is required in later steps.

Installing a Root CA Certificate on the Mobile Device

Copy the certificate file from the desktop PC to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.



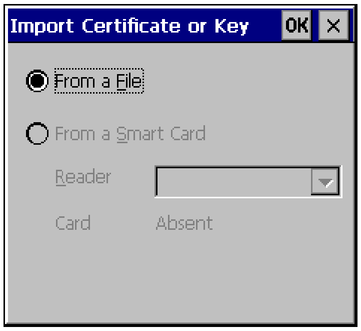
Trusted Authorities

Class 2 Public Primary Certification Authority
Class 3 Public Primary Certification Authority
Entrust.net Certification Authority (2048)
Entrust.net Secure Server Certification Authorit
Equifax Secure Certificate Authority
GlobalSign Root CA

Lists the certificates trusted by you

Figure 4-59 Certificates

Tap the "**Import**" button.



● From a File

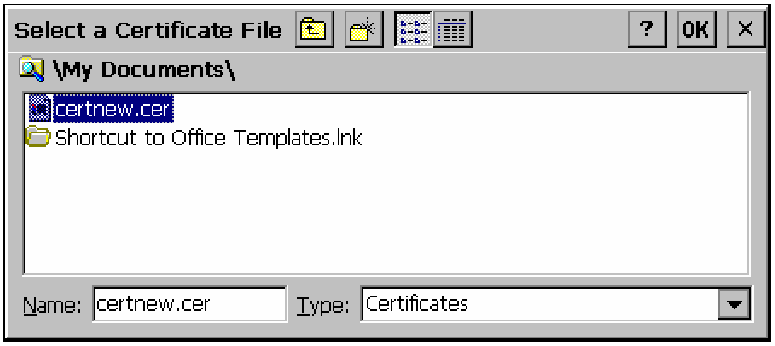
○ From a Smart Card

Reader

Card Absent

Figure 4-60 Import Certificate

Make sure "**From a File**" is selected and tap OK.



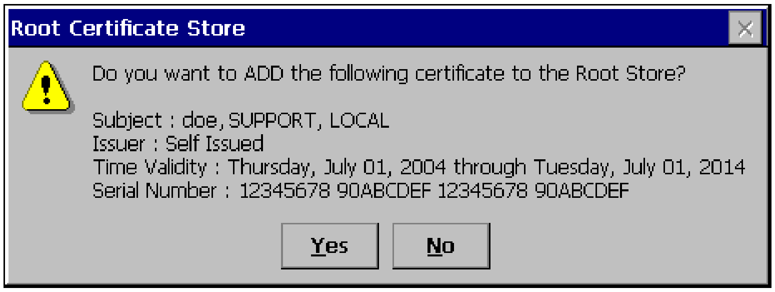
\My Documents\

certnew.cer
Shortcut to Office Templates.lnk

Name: certnew.cer Type: Certificates

Figure 4-61 Browsing to Certificate Location

Using the Explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.



Do you want to ADD the following certificate to the Root Store?

Subject : doe, SUPPORT, LOCAL
Issuer : Self Issued
Time Validity : Thursday, July 01, 2004 through Tuesday, July 01, 2014
Serial Number : 12345678 90ABCDEF 12345678 90ABCDEF

Figure 4-62 Certificate Import Confirmation

Tap **Yes** to import the certificate.

Once the certificate is installed, return to the proper authentication section, described later in this chapter.

User Certificates

Date/Time	It is important that all dates are correct on the .NET computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Generating a User Certificate for the MX3-RFID

Please refer to the "LXE Security Primer" for more information on obtaining and installing user certificates.

The easiest way to get the user certificate is to use a browser on a PC to navigate to the CA. To request the user certificate, open a browser to

http://<CA IP address>/certsrv

Sign into the CA with the username and password of the person who will be logging into the mobile device.

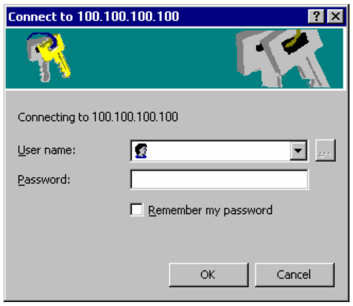
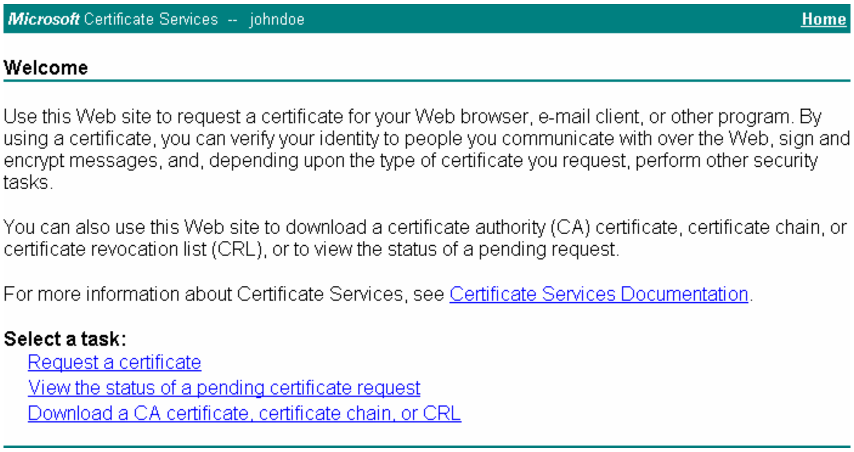


Figure 4-63 Logon to Certificate Authority

This process saves a user certificate and a separate private key file. CE .NET devices such as the MX3-RFID require the private key to be saved as a separate file rather than including the private key in the user certificate.



Microsoft Certificate Services -- johndoe   Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

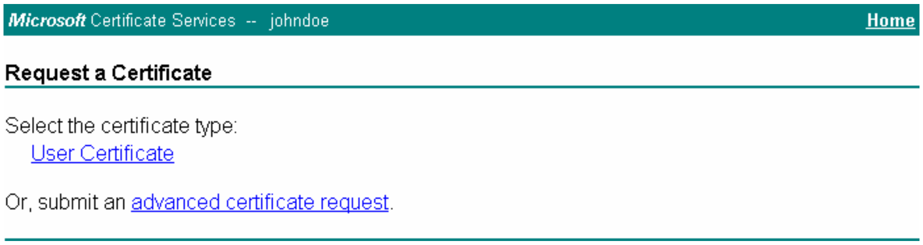
For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Figure 4-64 Certificate Services Welcome Screen

Click the "**Request a certificate"** task link.



Microsoft Certificate Services -- johndoe

Home

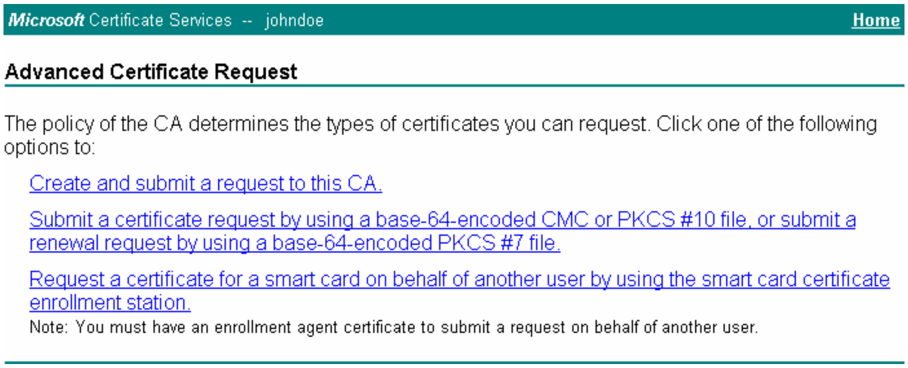
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Figure 4-65 Request a Certificate Screen

Click on the "**advanced certificate request"** link.



Microsoft Certificate Services -- johndoe

Home

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

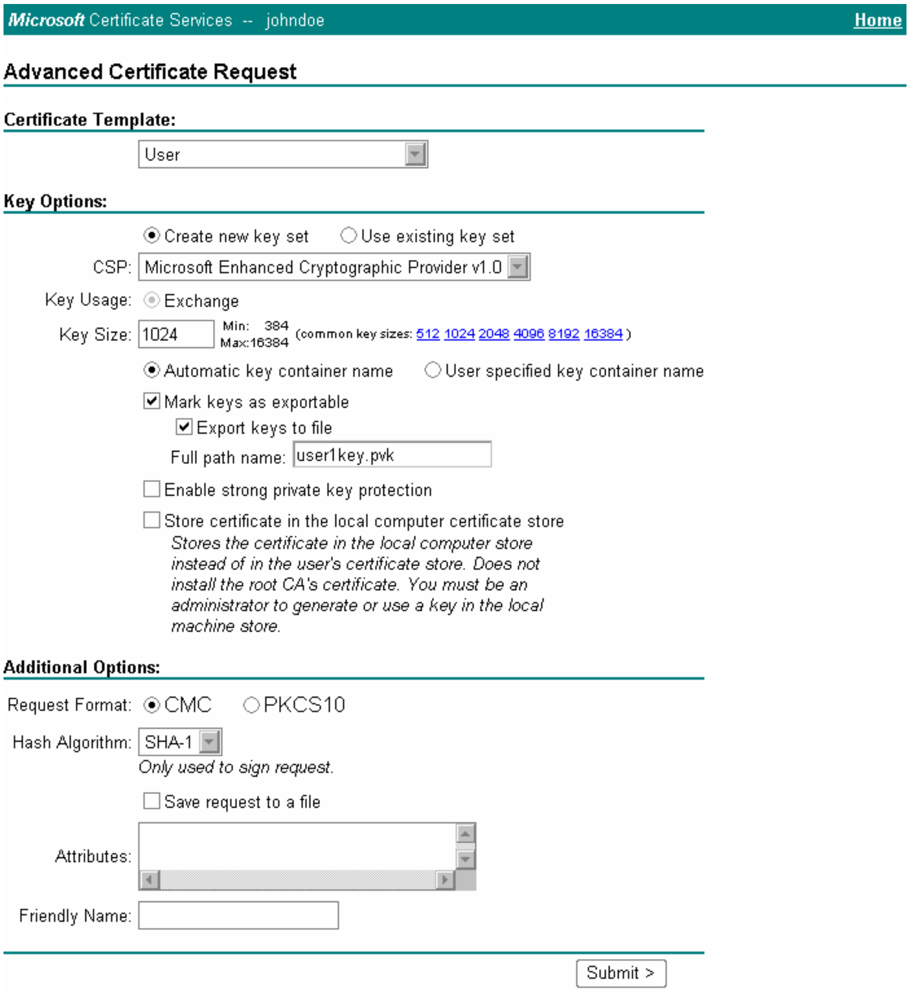
Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Figure 4-66 Advanced Certificate Request Screen

Click on the "**Create and submit a request to this CA"** link.



Microsoft Certificate Services -- johndoe **Home**

Advanced Certificate Request

Certificate Template:

User

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ● Exchange

Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

☑ Export keys to file

Full path name: user1key.pvk

☐ Enable strong private key protection

☐ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

☐ Save request to a file

Attributes:

Friendly Name:

Figure 4-67 Advanced Certificate Details

For the Certificate Template, select “User”.

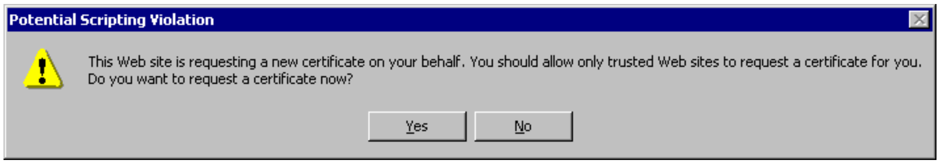
Check the “Mark keys as exportable” and the “Export keys to file” checkboxes.

Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

⚠	Be sure to note the name used for the private key file, for example RFIDUSER.PVK. The certificate file created later in this process must be given the same name, for example, RFIDUSER.CER.

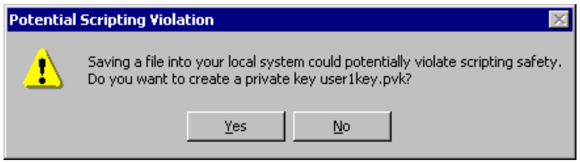
DO NOT check “Enable strong private key protection”.

Make any other desired changes and click the “Submit” button.



Potential Scripting Violation

This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

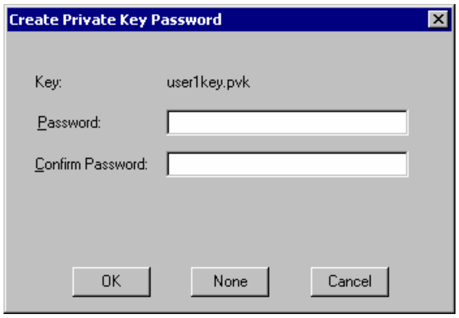


Potential Scripting Violation

Saving a file into your local system could potentially violate scripting safety. Do you want to create a private key user1key.pvk?

Figure 4-68 Script Warnings

If any script notifications occur, click the “Yes” button to continue the certificate request.



Create Private Key Password

Key: user1key.pvk

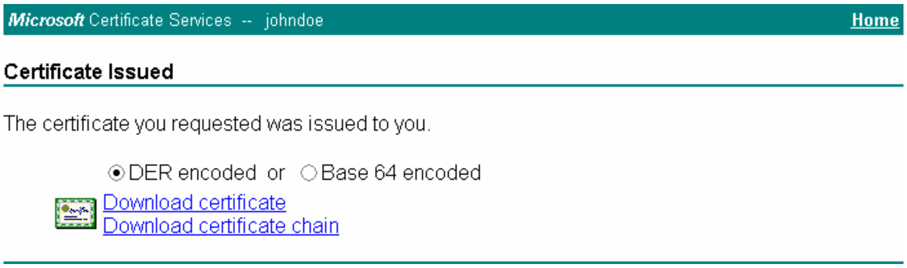
Password:

Confirm Password:

Figure 4-69 Script Warnings

When prompted for the private key password:

- Click “None” if you do not wish to use a password, *or*
- Enter and confirm your desired password then click “OK”.



Microsoft Certificate Services -- johndoe

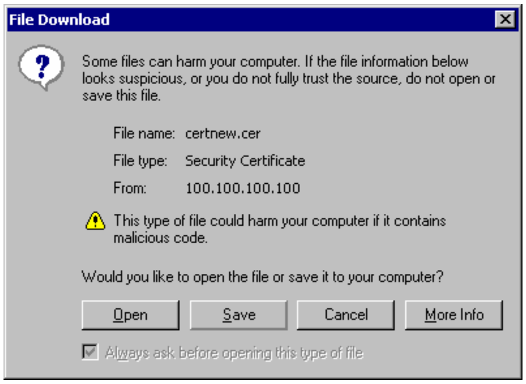
Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Figure 4-70 Certificate Issued

Click the **Download certificate** link.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certnew.cer

File type: Security Certificate

From: 100.100.100.100

This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

Figure 4-71 Download Security Warning

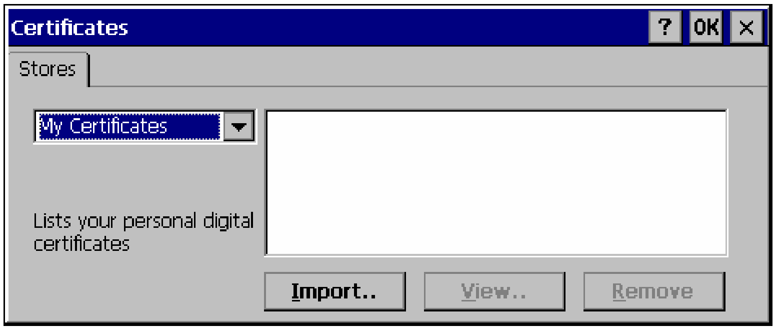
Click **Save** to download and store the user certificate to the PC. Keep track of the name and location of the certificate as the file name and location is required in later steps. The private key file is also downloaded and saved during this process.

⚠	Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as RFIDUSER.PVK then the certificate file created must be given the same name, for example, RFIDUSER.CER.

Installing a User Certificate on the Mobile Device (WPA-TLS Only)

Copy the certificate and private key files to the mobile device. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Select “My Certificates” from the pull down list.

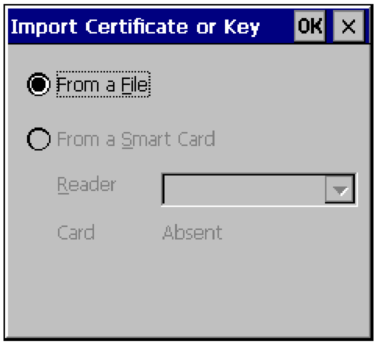


My Certificates

Lists your personal digital certificates

Figure 4-72 Certificates

Click the “Import” button.



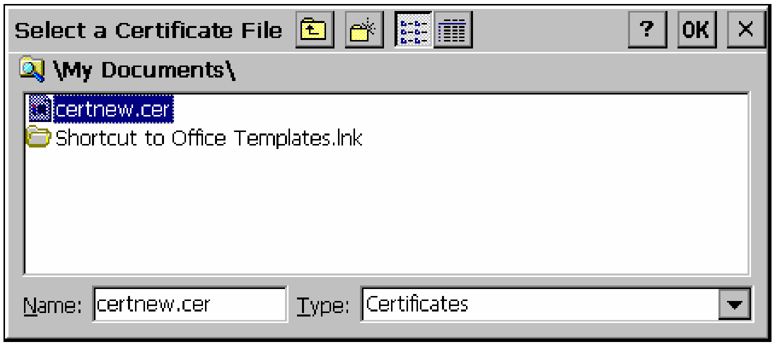
● From a File

○ From a Smart Card

Card Absent

Figure 4-73 Import Certificate

Make sure “From a File” is selected and click OK.



Select a Certificate File

\My Documents\

certnew.cer

Shortcut to Office Templates.lnk

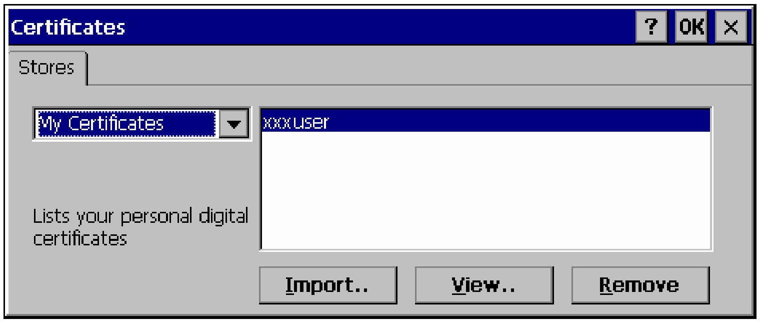
Name: certnew.cer

Type: Certificates

Figure 4-74 Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap OK.

The certificate is now shown in the list.



Certificates

Stores

My Certificates

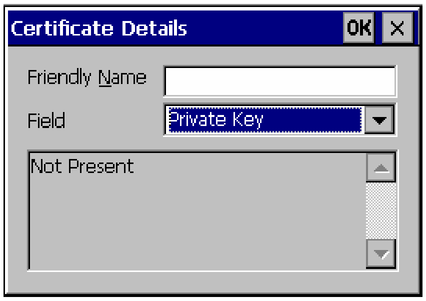
xxxuser

Lists your personal digital certificates

Figure 4-75 Certificate Listing

Highlight the certificate you just imported and tap the View. . button.

From the Field pull down menu, select "Private Key.



Certificate Details

Friendly Name

Field: Private Key

Not Present

Figure 4-76 Private Key Not Present

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap OK to return to the Certificates screen.

Tap import.

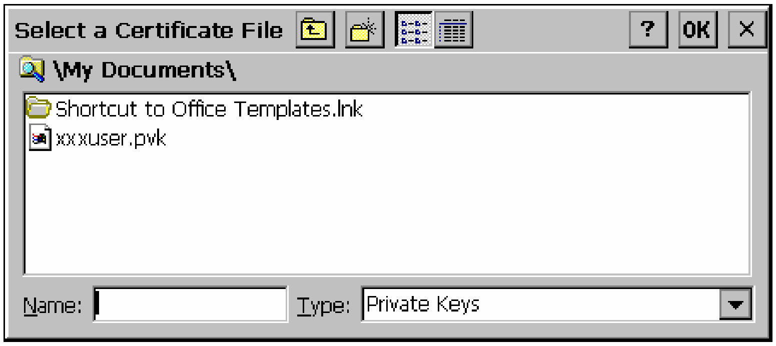


Figure 4-77 Browsing to Private Key Location

Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to "Private Keys", select the certificate desired and tap OK. Enter the password for the certificate if appropriate.

Tap View to see the certificate details again.

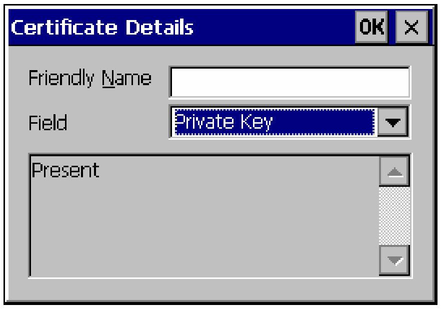


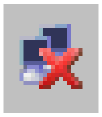
Figure 4-78 Private Key Present

The private key should now say "Present". If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example rfiduser.cer for the certificate and rfiduser.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

Wireless Zero Config Utility

Summit Client



Wireless Zero Config Icon

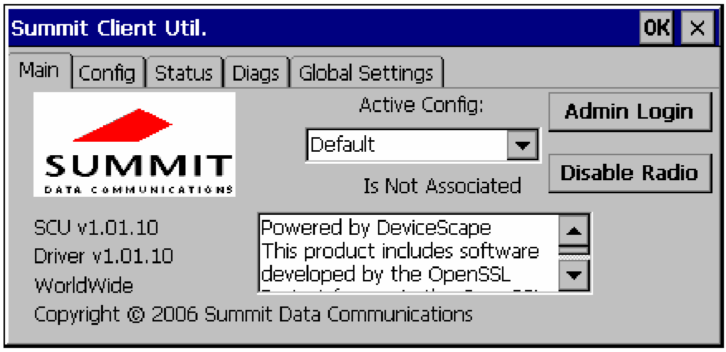
The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled and the MX3-RFID is not connected to a network.

LXE does not recommend use of the Wireless Zero Configuration Utility for configuring the radio as it cannot be used to configure all supported security protocols.

You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network.

LXE recommends using the Summit Client Utility to manage the radio.

To use Wireless Zero Config, first open the Summit Client Utility.



Active Config: Default

Is Not Associated

SCU v1.01.10

Driver v1.01.10

WorldWide

Powered by DeviceScape
This product includes software
developed by the OpenSSL

Copyright © 2006 Summit Data Communications

1. Select **ThirdPartyConfig** in the Active Config drop down box.
2. A message appears that a Power Cycle is required to make settings activate properly. Tap **OK**.
3. Tap the **Disable Radio** button to remove the connection to the Summit Client Utility. The text on the button changes to Enable Radio.
4. Tap the **Power** button to place the MX3-RFID in **Suspend**, then tap the Power button to **wake the MX3-RFID** from Suspend mode.

The Wireless Zero Config utility begins.

Appendix A Key Maps

Keypad

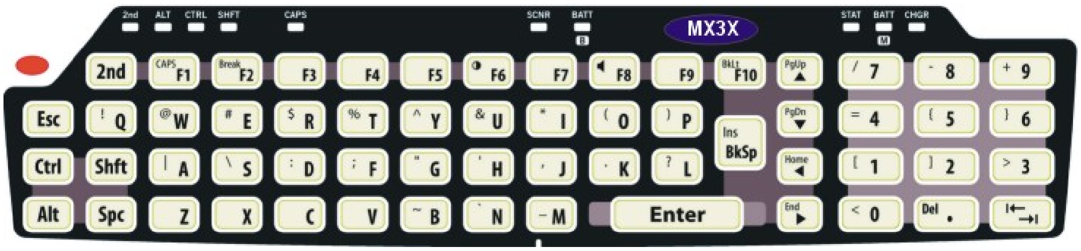


Figure A-1 QWERTY Keypad

Note: The key mapping in this appendix relates to the physical keypad. See section titled "Input Panel" for the Virtual (or Soft) Keypad used with the stylus.

Key Map 101-Key Equivalencies

Note: This key mapping is used on hand held computers that are NOT running an LXE Terminal Emulator.

When using a sequence of keys that includes the 2nd key, press the 2nd key first then the rest of the key sequence.

Note: When the computer boots, the default condition of NumLock is On and the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with a 2nd+F1 key sequence. The CAPS LED is illuminated when CapsLock is On.

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
Contrast	x					F6
Volume	x					F8
Backlight	x					F10
2nd						2nd
Shift						Shft
Alt						Alt
Ctrl						Ctrl
Esc						Esc
Space						Spc
Enter						Enter
Scan [3]						Scan

[3] Left Scan key default value is Scan. Right Scan key default value is Enter. When RFID Module is installed, Right Scan key defaults to RFID Read and Left Scan key defaults to Scan or Enter or Field Exit (5250 only).

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
CapsLock (Toggle)	x					F1
Back Space						BkSp
Tab						Tab
BackTab	x					Tab
Break	x					F2
Pause	x	x				F3
Up Arrow						Up Arrow
Down Arrow						Down Arrow
Right Arrow						Right Arrow
Left Arrow						Left Arrow
Insert	x					BkSp
Delete	x					DOT
Home	x					Left Arrow
End	x					Right Arrow
Page Up	x					Up Arrow
Page Down	x					Down Arrow
ScrollLock	x	x				F4
F1						F1
F2						F2
F3						F3
F4						F4
F5						F5
F6						F6
F7						F7
F8						F8
F9						F9
F10						F10
F11	x	x				F1
F12	x	x				F2
a					Off	A
b					Off	B
c					Off	C
d					Off	D
e					Off	E
f					Off	F
g					Off	G

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
h					Off	H
i					Off	I
j					Off	J
k					Off	K
l					Off	L
m					Off	M
n					Off	N
o					Off	O
p					Off	P
q					Off	Q
r					Off	R
s					Off	S
t					Off	T
u					Off	U
v					Off	V
w					Off	W
x					Off	X
y					Off	Y
z					Off	Z
A		x				A
B		x				B
C		x				C
D		x				D
E		x				E
F		x				F
G		x				G
H		x				H
I		x				I
J		x				J
K		x				K
L		x				L
M		x				M
N		x				N
O		x				O
P		x				P
Q		x				Q

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
R		x				R
S		x				S
T		x				T
U		x				U
V		x				V
W		x				W
X		x				X
Y		x				Y
Z		x				Z
1						1
2						2
3						3
4						4
5						5
6						6
7						7
8						8
9						9
0						0
DOT						DOT
<	x					0
[	x					1
]	x					2
>	x					3
=	x					4
{	x					5
}	x					6
/	x					7
-	x					8
+	x					9
*	x					I
: (colon)	x					D
; (semicolon)	x					F
?	x					L
`	x					N
_ (underscore)	x					M

To get this key	Press These Keys and Then					Press this key
	2nd	Shift	Ctrl	Alt	CapsLock	
, (comma)	x					J
‘ (apostrophe)	x					H
~ (tilde)	x					B
\	x					S
|	x					A
“	x					G
!	x					Q
@	x					W
#	x					E
$	x					R
%	x					T
^	x					Y
&	x					U
(	x					O
)	x					P

Creating Custom Key Maps

Prerequisite: LXE SDK CD

Introduction

A command-line compiler called KEYCOMP.EXE is provided on the SDK CD. Using this compiler, the System Administrator can convert a sample default key map text file into a custom key map text file which, when loaded onto the mobile device, can be chosen by the user to replace the default mobile device keymap and then switched back when they are finished using the customized keys. This custom key map file can be made to re-define the system return code for each of the 61 keys, key press or key press combinations. All keys, except the power key, can be re-mapped.

Custom keymaps for the mobile device are created on a desktop PC using the command line compiler KEYCOMP.EXE. Keycomp processes the input keymap source file and outputs a registry text file.

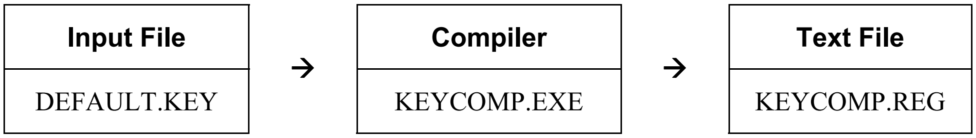
Note: Each VK_code has a numeric value (for example, VK_F20 = hex 83), these are documented in the SDK include file WINUSER.H (from Microsoft). The numeric value is what needs to go into the registry. Whether the value is hex or decimal depends on the registry editor being used - the one in the mobile device requires decimal, but the desktop one used over ActiveSync that a developer may use requires hex.

For Example

Default values: ScanCodeLeft = hex 83, decimal 131
ScanCodeRight = hex 84, decimal 132

Example:

KEYCOMP DEFAULT.KEY (writes KEYCOMP.REG to local directory)



Input File
DEFAULT.KEY
→
Compiler
KEYCOMP.EXE
→
Text File
KEYCOMP.REG

This output file should be renamed to **xxx.REG** (the suffix must remain REG), then copied to the mobile device over ActiveSync. Once the file is loaded on the mobile device, double-tap the file from the Windows CE Explorer desktop. This will run the REGLOAD utility to put it into the registry, and save the registry to non-volatile flash. The keymap is now a permanent part of the mobile device, and the REG file is no longer needed unless it is necessary to perform a cold boot; this will return the registry to factory defaults, and it will be necessary to double-tap the REG file again.

Once the keymap has been added to the registry, it should appear in the Keyboard control panel as the name given in the MAPNAME field in the key file. To activate the keymap, select the keymap from the popup menu, and close the control panel with the OK button. To return to the default keymap, select **0409** from the keymap popup and tap OK.

The compiler has three functional stages:

- First, the input file is read and parsed for any syntax errors. The data read is stored in internal tables.
- Second, the data parsed from the input file is validated to see that all of the items required by the keyboard driver for normal operation are present.

- Third and finally, the KEYCOMP.REG file is written out in the format required by the REGLOAD utility on the Windows CE device.

Programmable Scan Buttons and Custom Key Mapping

The Left and Right Scan buttons can be reset using Custom Key Mapping. Custom keymapping changes the placement of the buttons (e.g., F1 can now be Scan Left).

The keycode that the Scan Left (or F1) button generates is then determined by the setting in the scanner control panel (See Chapter 4 "System Configuration", Control Panel", "Scanner").

Remapping does not allow multiple entries. If the System Administrator uses Custom Key Mapping set a Scan button to ENTER, the original ENTER key must be redefined to something else. However, if the scanner control panel is used to change the Scan button to generate an ENTER, the original ENTER key is maintained as well.

Note: Tethered scanners are not activated/affected by the Scan buttons on the mobile device.

Keymap Source Format

The source file **DEFAULT.KEY** is supplied with the keymap compiler. This is the commented source for the default keymap **0409**. The comments in this file should make the majority of this document redundant. There is a copy of this file at the end of this section, in "Sample Input File**"**. This section should be read while referring to this sample source, for simplicity.

Note: You must change the name of the default key map from 0409 to some other number (i.e. 0509). To do this, change line #13 "MAPNAME=0409" to "MAPNAME=0509".

It is an important limitation that the keymap must have a 4, 5, or 6 digit numeric name; this is a limit of the Microsoft Windows CE layout manager.

The format of this file is familiar to anyone who has used .INI files under Windows. There is a section header in square brackets, followed by various values in the form *value=data*.

Lines beginning with a semicolon (;) or empty lines are ignored as comments. Spaces or tabs before or after the information are stripped off and ignored. Case is ignored in section names, value names, and value data.

*Note: Before connecting to a host using Remote Desktop Connection, go to **Start | Settings | Control Panel | Keyboard** and select **0409** from the keymap popup. Tap OK.*

COLxROWx Format

Note: There is no relationship between the physical layout COL/ROW of the keyboard / keypad and the COL/ROW listing in the key map file. The key map file represents the electrical layout not the physical layout.

All keys are specified in COLxROWx format. In this format, the first x is the 1 or 2 digit column in the keymap, and the second x is the 1 or 2 digit row in the keymap. All rows and columns are enumerated starting with zero (0).

In the **MAP** section, the **COLxROWx** is the value name, and the values must be less than the **MAPROWS** and **MAPCOLS** specified in the **GENERAL** section.

In the **SPECIAL** section, the **COLxROWx** is the value data, and the values given can be outside the normal key map limits.

GENERAL Section

The first section is the **GENERAL** section. This contains the keymap name (all numerics), as well as the number of rows and columns in the keymap, and the algorithm for converting rows and columns to a data byte to go into the keymap table.

```
.
[General]
MAPNAME=0409
MAPCNT=4
.
```

MAPNAME	Name of this map. This is what appears in the popup menu in the keyboard control panel.
MAPCNT	Gives the number of MAP sections (and hence keymap tables) in this source file.
MAPCOLS	Number of columns in each keymap table. This is defined by the hardware keyboard.
MAPROWS	Number of rows in each keymap table. This is defined by the hardware keyboard.
ALGOR	Defines the algorithm for converting row/column to internal scan code. Current values are: MX3X scancode = ((column << 3) + row)

Note: You must change the name of the default key map from 0409 to some other number (i.e. 0509). To do this, change line #13 "MAPNAME=0409" to "MAPNAME=0509".

SPECIAL Section

```
.
[Special]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
.
```

The second section is the **SPECIAL** section, which contains the row and column definitions for certain modifier keys which must be processed independent of the overall keymap. Currently, these are only modifier keys.

The only recognized names are: **KEYSHIFT**, **KEYALT**, **KEY2ND**, and **KEYCONTROL**, and these specify the row and column of these 4 specific modifier keys, in COLxROWx format. Note the row and column for these keys can be outside the keymap limits specified in the **GENERAL** section, since these are not loaded as part of the keymap proper.

MAP Section

```
.
[Map]
MAP=MAP_NORMAL
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
.
```

There will be several (4 to 7) **MAP** sections, each defining the keymap for a given combination of modifier keys. The keyboard driver requires keymaps for normal (no modifiers), SHIFT only, 2ND only, and 2ND-SHIFT combined.

The CTRL modifier and ALT modifier do not have individual keymaps; the keystrokes are passed to the operating system, which is allowed to parse these keys according to Microsoft specifications (for example, ALT-keys are defined to only pulldown menus, with no other function).

The only recognized value names are **MAP** and **COLxROWx** (defining a key code). The only valid values for **MAP** are:

MAP_NORMAL	no modifier keys
MAP_2ND	2nd modifier only
MAP_SHIFT	shift modifier only
MAP_2NDSHF (or) MAP_2NDSHIFT	2nd and shift modifiers together

In addition, certain keymaps are used for special adjustment functions within the keyboard driver, via the **CHANGE+mapname** specification:

MAP_VOLUM (or) MAP_VOLUME	special keymap for volume adjustment
MAP_CONTR (or) MAP_CONTRAST	special keymap for contrast adjustment
MAP_BRITE (or) MAP_BRIGHT	special keymap for brightness adjustment

When these maps are selected, the keyboard driver handles the up arrow and down arrow as adjusting the particular parameter up and down, and any other key exits the adjustment state. Keys in these modes are handled completely inside the keyboard driver, and are not propagated to the operating system.

Key codes are defined by **COLxROWx=scancode**. **Scancode** has a number of options, as follows:

VK_code	any valid Windows VK code (see below for valid codes)
'x'	a single ASCII character ('A','b','1','@',' ', etc.)
SHIFT+VK_code	for a shifted VK code (see below for valid codes)
SHIFT+'x'	for a shifted ASCII character (should not be needed)
ACTION+code	special function key (valid codes listed below)
CHANGE+mapname	for modifier keys, change keymaps to mapname, as specified above
OPEN	an unused key position, does nothing when pressed

Valid **ACTION** codes are as follows:

SCAN1	Scan key 1 (left side of screen on mobile device)
SCAN2	Scan key 2 (right side of screen on mobile device)
SCAN3	Handle trigger button (unused on mobile device, but specified)
POWER	power button
BACKLIGHT	backlight on/off function

Note that specifying the power button in a different location will affect suspend/resume functions. The "15-second hold to force reboot" function is controlled by hardware, and will only work with the default power button.

Keycomp Error Messages

Most error messages will specify the line within the keymap source file where the error occurred.

Duplicate key

A COLxROWx code was found in a MAP table, but that COL/ROW already has a value assigned.

GENERAL section must come before MAP

The GENERAL section must come first, or at least before any MAP sections. The GENERAL section defines parameters which are needed to process Maps

Header line missing close bracket

The section header line must have square brackets before and after the section name

Header line missing open bracket

The section header line must have square brackets before and after the section name

Invalid ACTION code %s

The key scan code is specified as ACTION+code, but the ACTION code parsed is not recognized. The following values are valid: SCAN1, SCAN2, SCAN3, POWER, or BACKLIGHT.

Invalid keycode %s

The keycode parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A' or '#').
- OPEN for unused entries (will not do anything when pressed)

Invalid MAP value %s

The MAP value parsed is not one the following list: MAP_NORMAL, MAP_2ND, MAP_SHIFT, MAP_2NDSHF, MAP_2NDSHIFT, MAP_VOLUM, MAP_VOLUME, MAP_CONTR, MAP_CONTRAST, MAP_BRITE, or MAP_BRIGHT.

Invalid MAPCNT (1-%d valid)

The specified MAPCNT exceeds the limits of the KEYCOMP compiler.

Invalid MAPCOLS (1-%d valid)

The specified MAPCOLS exceeds the limits of the KEYCOMP compiler.

Invalid MAPROWS (1-%d valid)

The specified MAPROWS exceeds the limits of the KEYCOMP compiler.

Invalid ROWCOL format

A COLxROWx was expected, but the format was not correct. The only valid formats are: COLxROWx, COLxxROWx, COLxROWxx, or COLxxROWxx, where xx are decimal numeric digits (0-9).

Invalid scan code

The scan code parsed is not recognized. The scan code can take one of the following formats:

- VK_code
- 'x'
- SHIFT+VK_code
- SHIFT+'x'
- ACTION+code
- CHANGE+mapname
- OPEN

Invalid section name %s

The section name parsed is invalid. The only recognized names are: GENERAL, SPECIAL, or MAP

Invalid SHIFT code %s

The key scan code is specified as SHIFT+code, but the SHIFT code parsed is not recognized. The following values are valid:

- VK code from the VK code table (below)
- 'x' where x is an ASCII code (e.g. 'A', '3', or '#').

Invalid value %s in GENERAL section

The value name parsed is invalid for the GENERAL section. The recognized names are: MAPNAME, MAPCNT, MAPCOLS, MAPROWS, or ALGOR

Invalid value %s in MAP section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: MAP and COLxxx.

Invalid value %s in SPECIAL section

The value name parsed is not expected in the SPECIAL section. The only recognized names are: KEYSHIFT, KEYALT, KEY2ND, and KEYCONTROL.

Invalid VK_ code %s

The VK code parsed is not recognized. See the VK Code Table (below) for valid values.

Map ended without MAP value

The MAP section must contain a MAP value, so the data fields can be parsed.

MAPNAME must be all numerics

Because of limitations in Microsoft Layout Manager, the map name must be all numeric (4, 5, or 6 digits). The name parsed did not fit this limitation.

No definition for map MAP_2ND

There is no 2nd keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_2NDSHIFT

There is no 2nd-SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_NORMAL

There is no Normal keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for map MAP_SHIFT

There is no SHIFT keymap defined. The keyboard driver requires this keymap to be defined. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.key2nd

No 2ND modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyalt

No ALT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keycontrol

No CTRL modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keydnarrow

No down arrow definition was found The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keypower

No power key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan1

No Scan Key 1 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan2

No Scan Key 2 definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyscan3

No Trigger Button definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyshift

No SHIFT modifier key definition was found. The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No definition for MapHead.keyuparrow

No up arrow definition was found The keyboard driver requires this key to be defined somewhere in one of the keymaps. This message comes from the post-parse validation, so no line # is specified.

No equal in value line

A value line must be of the form *value=data*. A value line was expected, but there was no equal in it. *(or)* A comment line did not begin with a semicolon (;).

No MAPNAME defined

There is no map name defined. The keyboard driver requires this name to be able to load the keymap tables. This message comes from the post-parse validation, so no line # is specified.

Scan code algorithm required

A COLxROWx data value was found before any ALGOR statement. ALGOR algorithm is parsed to decide how to encode COLxROWx into a keymap value.

Too many maps for specified MAPCNT

There are more MAP sections defined that the MAPCNT field specified.

Unknown scan code algorithm

The ALGOR algorithm specified is not one that KEYCOMP understands.

Unrecognized scancode algorithm %s

The ALGOR algorithm specified is not one that KEYCOMP understands.

Value outside of section

A value (defined as *value=data*) is only valid within a section (defined as *[section]*). A value line was found when a section header line was expected.

Sample Input File

```
;;----------------------------------------------------
;; keymap file for MX3X default keyboard
;;----------------------------------------------------

;;----------------------------------------------------
;; general parms give the size of arrays
;; all numeric values are decimal
;; these numbers are validated with the data below
;; at compile time
;; MAPNAME must be all numerics
;;----------------------------------------------------
[General]
MAPNAME=0409
MAPCNT=4
MAPCOLS=8
MAPROWS=8
ALGOR=MX3X

;;----------------------------------------------------
;; special keys are accessed outside the map
;; this specifies the row and column
;; these should not need to change, but...
;;----------------------------------------------------
[Special]
KEYSHIFT=COL8ROW0
KEYALT=COL9ROW0
KEY2ND=COL10ROW0
KEYCONTROL=COL11ROW0

;;----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with no modifier
;;----------------------------------------------------
[Map]
MAP=MAP_NORMAL
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=VK_ESCAPE
COL0ROW1=VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F2
COL0ROW4=VK_F5
COL0ROW5=VK_F7
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0='Q'
COL1ROW1='9'
COL1ROW2=ACTION+SCAN3
COL1ROW3='T'
COL1ROW4='U'
COL1ROW5='4'
COL1ROW6='O'
```

```
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0='A'
COL2ROW1=open
COL2ROW2='D'
COL2ROW3='G'
COL2ROW4='J'
COL2ROW5='1'
COL2ROW6='L'
COL2ROW7='3'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=' '
COL3ROW1=open
COL3ROW2='X'
COL3ROW3='V'
COL3ROW4='N'
COL3ROW5='0'
COL3ROW6=VK_LEFT
COL3ROW7=VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=VK_F9
COL4ROW1='S'
COL4ROW2=VK_RIGHT
COL4ROW3='F'
COL4ROW4='H'
COL4ROW5='K'
COL4ROW6='2'
COL4ROW7=VK_UP
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1='Z'
COL5ROW2=VK_BACK
COL5ROW3='C'
COL5ROW4='B'
COL5ROW5='M'
COL5ROW6=VK_PERIOD
COL5ROW7=VK_DOWN
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=VK_F10
COL6ROW1='W'
COL6ROW2=VK_RETURN
COL6ROW3='R'
COL6ROW4='Y'
COL6ROW5='I'
COL6ROW6='5'
COL6ROW7='P'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0='E'
COL7ROW1=open
COL7ROW2=VK_F3
COL7ROW3=VK_F4
COL7ROW4=VK_F6
COL7ROW5='7'
COL7ROW6=VK_F8
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

```
;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only 2ND
;;-----------------------------------------------------
[Map]
MAP=MAP_2ND
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_CAPITAL
COL0ROW2=ACTION+POWER
COL0ROW3=SHIFT+VK_PAUSE
COL0ROW4=open
COL0ROW5=open
COL0ROW6=VK_HYPHEN
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=SHIFT+'1'
COL1ROW1=SHIFT+VK_EQUAL
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'5'
COL1ROW4=SHIFT+'7'
COL1ROW5=VK_EQUAL
COL1ROW6=SHIFT+'9'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=SHIFT+VK_BACKSLASH
COL2ROW1=open
COL2ROW2=SHIFT+VK_SEMICOLON
COL2ROW3=SHIFT+VK_APOSTROPHE
COL2ROW4=VK_COMMA
COL2ROW5=VK_LBRACKET
COL2ROW6=SHIFT+VK_SLASH
COL2ROW7=SHIFT+VK_PERIOD
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=VK_BACKQUOTE
COL3ROW5=SHIFT+VK_COMMA
COL3ROW6=VK_HOME
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=VK_BACKSLASH
COL4ROW2=VK_END
COL4ROW3=VK_SEMICOLON
COL4ROW4=VK_APOSTROPHE
COL4ROW5=VK_PERIOD
COL4ROW6=VK_RBRACKET
COL4ROW7=VK_PRIOR
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0=SHIFT+VK_RBRACKET
COL5ROW1=open
```

```
COL5ROW2=VK_INSERT
COL5ROW3=open
COL5ROW4=SHIFT+VK_BACKQUOTE
COL5ROW5=SHIFT+VK_HYPHEN
COL5ROW6=VK_DELETE
COL5ROW7=VK_NEXT
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=ACTION+BACKLIGHT
COL6ROW1=SHIFT+'2'
COL6ROW2=open
COL6ROW3=SHIFT+'4'
COL6ROW4=SHIFT+'6'
COL6ROW5=SHIFT+'8'
COL6ROW6=SHIFT+VK_LBRACKET
COL6ROW7=SHIFT+'0'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=SHIFT+'3'
COL7ROW1=open
COL7ROW2=open
COL7ROW3=open
COL7ROW4=CHANGE+MAP_CONTRAST
COL7ROW5=VK_SLASH
COL7ROW6=CHANGE+MAP_VOLUME
COL7ROW7=open

;;-----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with 2ND and SHIFT
;;-----------------------------------------------------
[Map]
MAP=MAP_2NDSHIFT
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=open
COL0ROW1=VK_F11
COL0ROW2=ACTION+POWER
COL0ROW3=VK_F12
COL0ROW4=open
COL0ROW5=open
COL0ROW6='8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=open
COL1ROW1='9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=open
COL1ROW4=open
COL1ROW5='4'
COL1ROW6=open
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=open
COL2ROW1=open
COL2ROW2=open
COL2ROW3=open
COL2ROW4=open
```

```
COL2ROW5='1'
COL2ROW6=open
COL2ROW7='3'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=open
COL3ROW1=open
COL3ROW2=open
COL3ROW3=open
COL3ROW4=open
COL3ROW5='0'
COL3ROW6=open
COL3ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=open
COL4ROW1=open
COL4ROW2=open
COL4ROW3=open
COL4ROW4=open
COL4ROW5=open
COL4ROW6='2'
COL4ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0='6'
COL5ROW1=open
COL5ROW2=open
COL5ROW3=open
COL5ROW4=open
COL5ROW5=open
COL5ROW6=open
COL5ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=open
COL6ROW1=open
COL6ROW2=open
COL6ROW3=open
COL6ROW4=open
COL6ROW5=open
COL6ROW6='5'
COL6ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=open
COL7ROW1=open
COL7ROW2=VK_PAUSE
COL7ROW3=VK_SCROLL
COL7ROW4=VK_SNAPSHOT
COL7ROW5='7'
COL7ROW6=open
COL7ROW7=open
;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

```
;;----------------------------------------------------
;; the name of this key doesn't matter
;; the important part is the MAP value
;; codes are defined in docs
;; this is the map for keys with only SHIFT
;;----------------------------------------------------
[Map]
MAP=MAP_SHIFT
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL0ROW0=SHIFT+VK_ESCAPE
COL0ROW1=SHIFT+VK_F1
COL0ROW2=ACTION+POWER
COL0ROW3=SHIFT+VK_F2
COL0ROW4=SHIFT+VK_F5
COL0ROW5=SHIFT+VK_F7
COL0ROW6=SHIFT+'8'
COL0ROW7=ACTION+SCAN1
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL1ROW0=SHIFT+'Q'
COL1ROW1=SHIFT+'9'
COL1ROW2=ACTION+SCAN3
COL1ROW3=SHIFT+'T'
COL1ROW4=SHIFT+'U'
COL1ROW5=SHIFT+'4'
COL1ROW6=SHIFT+'O'
COL1ROW7=ACTION+SCAN2
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL2ROW0=SHIFT+'A'
COL2ROW1=open
COL2ROW2=SHIFT+'D'
COL2ROW3=SHIFT+'G'
COL2ROW4=SHIFT+'J'
COL2ROW5=SHIFT+'1'
COL2ROW6=SHIFT+'L'
COL2ROW7=SHIFT+'3'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL3ROW0=SHIFT+' '
COL3ROW1=open
COL3ROW2=SHIFT+'X'
COL3ROW3=SHIFT+'V'
COL3ROW4=SHIFT+'N'
COL3ROW5=SHIFT+'0'
COL3ROW6=SHIFT+VK_LEFT
COL3ROW7=SHIFT+VK_TAB
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL4ROW0=SHIFT+VK_F9
COL4ROW1=SHIFT+'S'
COL4ROW2=SHIFT+VK_RIGHT
COL4ROW3=SHIFT+'F'
COL4ROW4=SHIFT+'H'
COL4ROW5=SHIFT+'K'
COL4ROW6=SHIFT+'2'
COL4ROW7=SHIFT+VK_UP
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL5ROW0=SHIFT+'6'
COL5ROW1=SHIFT+'Z'
```

```
COL5ROW2=SHIFT+VK_BACK
COL5ROW3=SHIFT+'C'
COL5ROW4=SHIFT+'B'
COL5ROW5=SHIFT+'M'
COL5ROW6=SHIFT+VK_PERIOD
COL5ROW7=SHIFT+VK_DOWN
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL6ROW0=SHIFT+VK_F10
COL6ROW1=SHIFT+'W'
COL6ROW2=SHIFT+VK_RETURN
COL6ROW3=SHIFT+'R'
COL6ROW4=SHIFT+'Y'
COL6ROW5=SHIFT+'I'
COL6ROW6=SHIFT+'5'
COL6ROW7=SHIFT+'P'
;;;;;;;;;;;;;;;;;;;;;;;;;;;
COL7ROW0=SHIFT+'E'
COL7ROW1=open
COL7ROW2=SHIFT+VK_F3
COL7ROW3=SHIFT+VK_F4
COL7ROW4=SHIFT+VK_F6
COL7ROW5=SHIFT+'7'
COL7ROW6=SHIFT+VK_F8
COL7ROW7=open
```

Sample Output File

```
[HKEY_CURRENT_USER\Keyboard Layout\0409]
;; header limits and special keys
;;  MAPCNT
;;  MAPCOLS
;;  MAPROWS
;;  # of keys in each map
;;  (unused)
;;  (unused)
;;  scancode value for power key
;;  scancode value for up arrow
;;  scancode value for down arrow
;;  scancode value for scan key 1
;;  scancode value for scan key 2
;;  scancode value for trigger button
;;  scancode value for SHIFT
;;  scancode value for ALT
;;  scancode value for 2ND
;;  scancode value for CTRL key
"Head"=hex: 04,08,08,40,00,00,02,27,2F,07,0F,0A,40,48,50,58

;; Map0 is the scancode values for the NORMAL key map
"Map0"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00

;; Flag0 is the shift codes for the NORMAL key map
"Flag0"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Map1 is the scancode values for the 2ND key map
"Map1"=hex:\
    00,14,DF,13,00,00,BD,87,31,BB,89,35,37,BB,39,88,\
    DC,00,BA,DE,BC,DB,BF,BE,00,00,00,00,C0,BC,24,09,\
    00,DC,23,BA,DE,BE,DD,21,DD,00,2D,00,C0,BD,2E,22,\
    8A,32,00,34,36,38,DB,30,33,00,00,00,00,BF,00,00

;; Flag1 is the shift codes for the 2ND key map
"Flag1"=hex:\
    00,00,A0,10,00,86,00,A0,10,10,A0,10,10,00,10,A0,\
    10,00,10,10,00,00,10,10,00,00,00,00,00,10,00,10,\
    00,00,00,00,00,00,00,00,10,00,00,00,10,10,00,00,\
    A0,10,00,10,10,10,10,10,10,00,00,00,85,00,84,00

;; Map2 is the scancode values for the 2ND-SHIFT key map
"Map2"=hex:\
    00,7A,DF,7B,00,00,38,87,00,39,89,00,00,34,00,88,\
    00,00,00,00,00,31,00,33,00,00,00,00,00,30,00,00,\
    00,00,00,00,00,00,32,00,36,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,35,00,00,00,13,91,2C,37,00,00

;; Flag2 is the shift codes for the 2ND-SHIFT key map
"Flag2"=hex:\
    00,00,A0,00,00,00,00,A0,00,00,A0,00,00,00,00,A0,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\
    00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00

;; Map3 is the scancode values for the SHIFT key map
"Map3"=hex:\
    1B,70,DF,71,74,76,38,87,51,39,89,54,55,34,4F,88,\
    41,00,44,47,4A,31,4C,33,20,00,58,56,4E,30,25,09,\
    78,53,27,46,48,4B,32,26,36,5A,08,43,42,4D,BE,28,\
    79,57,0D,52,59,49,35,50,45,00,72,73,75,37,77,00

;; Flag3 is the shift codes for the SHIFT key map
"Flag3"=hex:\
    10,10,A0,10,10,10,10,A0,10,10,A0,10,10,10,10,A0,\
    10,00,10,10,10,10,10,10,10,00,10,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,\
    10,10,10,10,10,10,10,10,10,00,10,10,10,10,10,00
```

List of Valid VK Codes for CE .NET

This is the list of codes parsed by KEYCOMP compiler. Refer to Microsoft Windows documentation for further clarification of the meaning of these key codes. Any VK keys not defined here are not valid for use under Windows CE .NET.

VK_ADD	VK_F3	VK_NUMPAD9
VK_APOSTROPHE	VK_F4	VK_OEM_CLEAR
VK_APPS	VK_F5	VK_OFF
VK_ATTN	VK_F6	VK_PA1
VK_BACK	VK_F7	VK_PAUSE
VK_BACKQUOTE	VK_F8	VK_PERIOD
VK_BACKSLASH	VK_F9	VK_PLAY
VK_BROWSER_BACK	VK_FINAL	VK_PRINT
VK_BROWSER_FAVORITES	VK_HANGUL	VK_PRIOR
VK_BROWSER_FORWARD	VK_HANJA	VK_RBRACKET
VK_BROWSER_HOME	VK_HELP	VK_RBUTTON
VK_BROWSER_REFRESH	VK_HOME	VK_RCONTROL
VK_BROWSER_SEARCH	VK_HYPHEN	VK_RETURN
VK_BROWSER_STOP	VK_INSERT	VK_RIGHT
VK_CANCEL	VK_JUNJA	VK_RMENU
VK_CAPITAL	VK_KANA	VK_RSHIFT
VK_CLEAR	VK_KANJI	VK_RWIN
VK_COMMA	VK_LAUNCH_APP1	VK_SCROLL
VK_CONTROL	VK_LAUNCH_APP2	VK_SELECT
VK_CONVERT	VK_LAUNCH_MAIL	VK_SEMICOLON
VK_CRSEL	VK_LAUNCH_MEDIA_SELECT	VK_SEPARATOR
VK_DECIMAL	VK_LBRACKET	VK_SHIFT
VK_DELETE	VK_LBUTTON	VK_SLASH
VK_DIVIDE	VK_LCONTROL	VK_SLEEP
VK_DOWN	VK_LEFT	VK_SNAPSHOT
VK_END	VK_LMENU	VK_SPACE
VK_EQUAL	VK_LSHIFT	VK_SUBTRACT
VK_EREOF	VK_LWIN	VK_TAB
VK_ESCAPE	VK_MBUTTON	VK_UP
VK_EXECUTE	VK_MEDIA_NEXT_TRACK	VK_VOLUME_DOWN
VK_EXSEL	VK_MEDIA_PLAY_PAUSE	VK_VOLUME_MUTE
VK_F1	VK_MEDIA_PREV_TRACK	VK_VOLUME_UP
VK_F10	VK_MEDIA_STOP	VK_ZOOM
VK_F11	VK_MENU	
VK_F12	VK_MULTIPLY	
VK_F13	VK_NEXT	
VK_F14	VK_NOCONVERT	
VK_F15	VK_NONAME	
VK_F16	VK_NUMLOCK	
VK_F17	VK_NUMPAD0	
VK_F18	VK_NUMPAD1	
VK_F19	VK_NUMPAD2	
VK_F2	VK_NUMPAD3	
VK_F20	VK_NUMPAD4	
VK_F21	VK_NUMPAD5	
VK_F22	VK_NUMPAD6	
VK_F23	VK_NUMPAD7	
VK_F24	VK_NUMPAD8	

Appendix B Technical Specifications

Physical Specifications

Features		Specifications	Comments	
CPU		Xscale PXA255 CPU operating at 400 MHz. Turbo mode switching is supported.	32 bit CPU (with on-chip cache)	
Compact Flash (Internal)		Supports an ATA interface only.	3.3v ATA flash card. Inaccessible by customer.	
Memory	ROM	64 MB Flash		
	RAM	64 or 128MB of SDRAM	System Memory	
Display	LCD	Transmissive Color with Touchscreen	Customer Configurable Backlighting	
Mass Storage	Removable PC Card	SRAM or Flash PCMCIA Type I or II PC Cards (Various Sizes) Compact Flash Card	Bootable SRAM PC Card, ATA Flash PC Card, or ATA Hard Drive PC Card (Customer Installable)	
PCMCIA Interface		Slot 0 accepts Type I and II Slot 1 accepts Type I and II CF+	Compatible with the PCMCIA version 2.1 standard.	
Weights		Unit with radio, battery and scanner endcap	Less than 30 oz	<850g 1128.3g for RFID
		Battery	5.6 oz	157g
		Radio Card - 2.4GHz Type II	1.0 oz 1.6 oz	28g 45g
		SRAM Card	1 oz	28g
External Connectors/Interface USB Host / Client Ports		IrDA Connector (COM 2) bi-directional half-duplex	Supports 115k baud	
		Endcap – incl Scanner (COM 3), DA-9 (COM 1)	Scanner – SE923 or SE955 Symbol engine	
Power Connector		8.5V - 15 VDC Input Power	External Battery Charger Contacts	
		10.8 - 16VDC Input Power	Power Jack	
Audio Connector			Audio Jack	
Dimensions w/Endcap		Length	6”	15 cm
		Width	8”	20 cm
		Depth (With RFID Module)	1.88”	4.77 cm

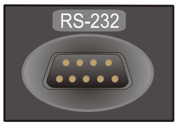
Features		Specifications	Comments
Batteries	Main	1900 mAh 10.8V, 3 cell, Li-Ion battery pack	In-Unit Chargeable or Externally Chargeable
	Backup (CMOS)	Internal Nickel-Cadmium (NiCd) 5.7V max.	Automatically charges from main battery during normal operation Memory operational for 5 minutes when main battery is depleted

Display Specifications

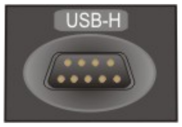
Type	LCD - Transmissive Color Electroluminescent Backlighting
Resolution	640x240 pixels
Size	½ VGA landscape
Diagonal Viewing Area	5.92 in (150.4mm)
Dot Pitch	0.22mm
Dot Size	0.20mm x 0.20mm
Color Scale	Transmissive – 256 colors

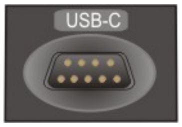
Cable Specifications

Caution: Do Not Use this Port for Cables with USB Plugs/Receptacles:

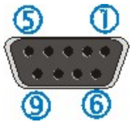
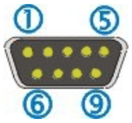


Caution: Do Not Use these Labeled Ports for Tethered Scanners:





Cable Ends

Receptacle	Plug	Receptacle	Plug
USB A	USB A	 RS232	 RS232
USB B	USB B		

Cable Pinouts and Diagrams

MX3XA069CBLD9USBCLNT – CBL, USB D9F to USB Type A Receptacle *ActiveSync*: Connect from mobile device USB-C port to USB Type A Host. E.g. laptop/desktop PC. 	Mobile Device Client End — Goes To — USB Type A Plug End 1........................ Host Detect .... 1 2........................ Not Used 3........................ D+ .... 3 4........................ Not Used 5........................ GND .... 4 6........................ Not Used 7........................ D- .... 2 8........................ Not Used 9 Not Used
MX3X068CBLD9USBHOST – CBL, USB D9F to USB Type B Plug Connect from USB-H port to USB Type B device. e.g. Hub, camera, other client device, etc. 	Mobile Device Host port End — Goes To — USB Type B Plug End 1........................ Not Used 2........................ Not Used 3........................ D+ .... 3 4........................ Not Used 5........................ GND .... 4 6........................ Not Used 7........................ D- .... 2 8........................ Not Used 9........................ PWR 1

Environmental Specifications

Mobile Device and Endcaps

Operating Temperature	32°F to 122°F (0°C to 50°C) color
Storage Temperature	-22°F to 158°F (-30°C to 70°C)
Water and Dust	IEC IP65
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Ambient Light – ranging from total darkness to direct sunlight	Display readable (with backlight on) for <= two hours Keypad readable (after previous exposure to a 60W bulb for 30 minutes) for <= 15 minutes.
Contamination	Resistant to exposure to skin oil and other lubricants.
Vibration	Based on MIL Std 810F
ESD	8 KV air, 4kV direct contact
Shock, MX3X	Multiple 4 foot drops to concrete. 6 foot with protective cover/boot

Power Supplies

US AC Wall Adapter

Input Power Switch	None
Power "ON" Indicator	None
Input Fusing	Thermal Fuse
Input Voltage	108VAC min - 132VAC max
Input Frequency	47 - 63 Hz
Input Connector	North American wall plug, no ground
Output Connector	Barrel connector, female, 5.5 x 2.5 x 11.5mm, Center Positive
Output Voltage	+12VDC, unregulated
Output Current	0 Amps min, 1.5 A max
Operating Temperature	32° F to 104° F / 0° C to 40° C
Storage Temperature	-13° F to 158° F / -25° C to 70° C
Humidity	Operates in a relative humidity of 5 – 95% (non-condensing)

International AC Adapter

Operating Temperature	32°F to 104°F (-0°C to 40°C)
Storage Temperature	-13°F to 158°F (-25°C to 70°C)
Operating Humidity	Up to 90% non-condensing at 104°F (40°C)
Input Power Switch	None
Power "ON" Indicator	None
Input Voltage	108VAC min - 264VAC max
Input Frequency	47 - 63 Hz
Input Connector	Customer supplied
Output Connector	Barrel connector, female, 5.5 x 2.5 x 11mm, Center Positive
Output Voltage	+12VDC, regulated
Output Voltage Regulation	+/- 5%
Output Current	0 Amps min, 1.00 Amps max

Radio Specifications

Summit Client in PCMCIA Adapter Card 2.4GHz Type II

Bus Interface:	Compact Flash via a PCMCIA adapter
Radio Frequencies:	2.4 - 2.4897 GHz IEEE 802.11b 802.11g DSSS OFDM
RF Data Rates:	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level:	18 dBm 64mW Max
Channels	11 US, 13 Europe, 13 Japan
Operating Temperature	see MX3-RFID Environmental Specs
Storage Temperature	see MX3-RFID Environmental Specs
Connectivity:	Novell, TCP/IP, Ethernet, ODI

Cisco Client PCMCIA Card 2.4GHz Type II

Bus Interface	PCMCIA 2.0, Type II slot
Radio Frequencies	2.4 - 2.4835 GHz IEEE 802.11b DS SS
RF Data Rates	11 Mbps
RF Power Level	100 mW max.
Channels	11 US, 13 Europe, 4 France, 14 Japan
Operating Temperature	see MX3-RFID Environmental Specs
Storage Temperature	see MX3-RFID Environmental Specs
Connectivity	Novell, TCP/IP, Ethernet, ODI
Antenna	Internal

Index